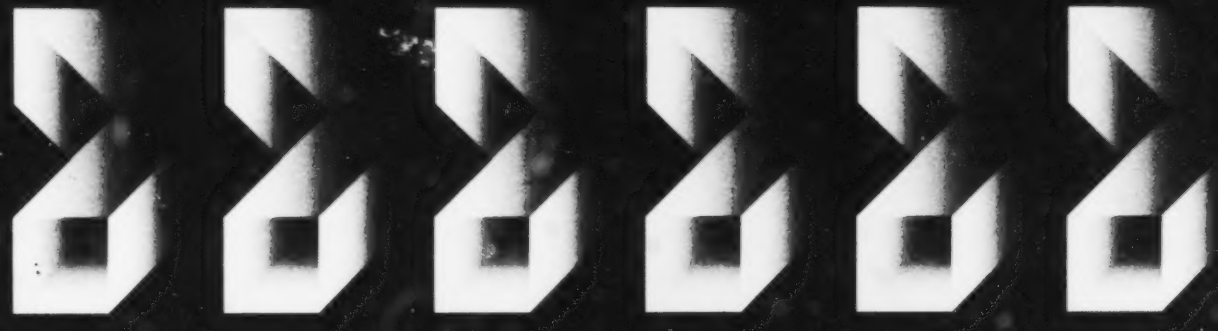
Health Canada Santé Canada

Audit and Accountability Bureau

Bureau de la vérification et de la responsabilisation



INTERNAL AUDIT REPORT

Controls and Security for Interactive Leave and Attendance Module (ILAM)

December 15, 1999

Canada

103-05697/

INTERNAL AUDIT REPORT

Controls and Security for Interactive Leave and Attendance Module (ILAM)

December 15, 1999

Audit conducted
by the
Internal Audit Directorate
Health Canada

Audit Number
A8113

Audit Chronology

- Audit examinations started — October 4,1999
- Audit examinations completed — October 25, 1999
- Draft audit report accepted by the Senior Assistant Deputy Minister, Corporate Services Branch — December 9, 1999
- Final audit report approved by the Chair, Departmental Audit and Evaluation Committee — December 15, 1999

credits

This audit was conducted by **PricewaterhouseCoopers (PwC)** under the direction of the Internal Audit Directorate. The departmental project manager was **Carolyn Jeffrey**, under the general direction of **Gordon Peters,** Director, Internal Audit. The members of the **PwC** audit team and their roles were as follows:

David Prime, PwC Principal Consultant, was the audit team leader.

Lana Doxtator, PwC Sr Team Member, conducted the audit in the NCR.

Valerie Plaskacz, PwC Sr. Team Member, reviewed the ILAM process in the Montreal test location.

Contents

	Page
INTRODUCTION	1
Background	1
Methodology and Audit Criterea	2
Overview and Status of ILAM	3
FINDINGS	4
Internal Controls	4
Recommendations	9
Security	10
Recommendations	12
APPENDIX A - CobiT Processes and Objectives And Observations and Assessments	
APPENDIX B - Corrective Action Plan Submitted by the Human Resources Directorate	

INTRODUCTION

Background

An Interactive Leave Attendance Module (ILAM) has been developed by the Human Resources Directorate of Health Canada to capture leave and attendance data in electronic form. ILAM is being developed primarily by the Departmental Network Applications Solutions (DNAS) group. Co-ordination and assistance is provided by:

i. the PMIS technical team;
ii. Production Control, for the linkages to PMIS; and
iii. ILAM business owner in the Human Resources Directorate, for functionality considerations.

The ILAM business owner asked the Internal Audit Directorate to conduct an audit in January 1999, to assess whether the essential controls were in place and working within the system. The audit report included several recommendations to address internal controls. The ILAM project team responded to the recommendations of this report in "Action Plan in Response to ILAM audit", updated as at September 10, 1999. The ILAM business owner requested the Internal Audit Directorate to conduct a second audit in October 1999.

The objectives of this audit were to independently review, assess and report on the integrity of the module and security issues in the following context:

- The ability of the current version of the module and the links to Lotus Notes and the Personnel Management Information System to perform as intended; and
- The security of the application from unauthorized access and data manipulation.

The review focused on ILAM and the links to PMIS and the Oracle database. The scope also included:

- The data process of the module, all electronic linkages, and output;
- The security aspects of access to and manipulation of the data;
- Retention of back-ups and ability to recover from failure

The audit addressed only application security and not the other security layers, e.g., the network, operating system, physical security and telecommunications.

The review was conducted within the Tunney's Pasture, Ottawa, location of Health Canada in October and November 1999.

During the audit, the ILAM pilot was ongoing. Pilot evaluations and testing results had not, as of November 1, 1999, been summarised and analysed by the ILAM business owner. However, we were able to review the summary results of the ILAM project team's detailed testing of the accuracy of ILAM/PMIS processing, done over a three day window from October 18, 1999 to October 29, 1999 (approximately 270 transactions). We were also able to review the test results documented in the ILAM Acceptance Testing Log.

Methodology and Audit Criteria

The study was conducted through:

- Discussions with Human Resources staff (the ILAM business owners) and the ILAM/PMIS technical project leaders, including some from the Montreal pilot team;
- A review of relevant project documentation; and
- Observation of a demonstration of the internal controls and security functionality designed into ILAM as at October 1999 at NCR[1].

The Control Objectives for Information and Related Technology (CobiT) framework developed by the Information Systems Audit and Control Foundation (ISACF) was used to develop audit criteria. Five audit criteria from two CobiT Process areas were included in this review:

CobiT Process Area	CobiT Criteria	CobiT High-level Control Objective
Delivery & Support	**DS4**: Ensure continuous service	IT services should be available as required and ensure a minimum business impact in the event of a major disruption by having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements.
Delivery & Support	**DS5**: Ensure systems security	Information should be safeguarded against unauthorised use, disclosure or modification, damage or loss by logical access controls which ensure access to systems, data and programmes are restricted to authorised users.
Delivery & Support	**DS10**: Manage problems and incidents	Problems and incidents should be resolved, and the cause investigated by a problem management system, which records and progresses all incidents.
Delivery & Support	**DS11**: Manage data	Data should remain complete, accurate and valid during its input, update and storage through an effective combination of application and general controls over IT operations.
Monitoring	**M2**: Assess internal control adequacy	Internal control objectives set for the IT processes should be achieved by management's commitment to monitoring internal controls, assessing their effectiveness and reporting on them on a regular basis.

The detailed audit criteria and objectives are presented in ***Appendix A***.

---

[1] We attempted to observe a demonstration of ILAM at the Montreal pilot location on November 1, 1999, but due to server problems at the Montreal office, the office was unable to carry out the demonstration.

Report Organization

This report is organized into two sections: Overview and status of ILAM; and Findings. The Findings section includes two categories: Internal Control (including back-ups and the ability to recover from failure); and Security.

Detailed observations and our assessment of the internal controls and security against the CobiT criteria of ILAM are presented in the table in ***Appendix A***.

OVERVIEW AND STATUS OF ILAM

ILAM, a Lotus Notes based application, will support on-line input of leave applications by all Health Canada employees who have access to Lotus Notes. Initial set up of ILAM for each employee requires the employee to access Lotus Notes through input of his/her Notes password, and input of his/her PRI (Health Canada unique identifier) and birthdate. The PRI and birthdate is validated in ILAM against information downloaded from PMIS. Once the employee has created his/her ILAM profile, subsequent access to the employee's ILAM information is available once the employee has logged on to Lotus Notes. The employee may log on at any time to review the details of leave transactions, as well as leave balances.

Requests for leave are created by the employee and forwarded for approval to the assigned supervisor. Employees cannot approve their own requests. If an assigned supervisor has previously approved or rejected an employee's leave request, the supervisor may input a leave request on behalf of the employee and forward the request to another supervisor for approval. The employee is informed of this transaction by ILAM generated e-mail.

Supervisors are selected by the employee. There are no checks within ILAM or PMIS to validate the legitimacy of the supervisor. Once an initial supervisor has been assigned, the employee may again select an alternate supervisor. The initial supervisor (who may or may not be the legitimate supervisor) is not informed by ILAM of the change. Each supervisor has access only to the transactions he/she approved (or recommended) for the employee.

Approved requests for Leave With Pay (LWP), for current year, will be electronically transmitted to PMIS on a nightly basis. The updated PMIS data will be downloaded nightly to refresh the ILAM databases. If PMIS rejects a request approved in ILAM, the employee receives an error message. Approved requests for the next fiscal period will be held in a separate ILAM file for PMIS processing during the new year rollover process.

Approved requests for Leave Without Pay (LWOP) will be processed by Pay and Benefits in response to an ILAM generated e-mail message, sent to a unique Pay and Benefits mailbox set up for ILAM processing (accessible only to Pay and Benefits personnel). Update access rights to the mailbox is limited to Production staff and Pay and Benefit Managers, read access is provided to Pay and Benefit Officers, by pay list.

Requests (LWP and LWOP) that have not been approved do not remain in ILAM. After 15 days, a reminder message is sent to the originator and supervisor. After 20 days, the rejected request is deleted from ILAM. Any unactioned requests are deleted after 60 days.

The nightly PMIS/ILAM batch cycle will be monitored and controlled by Production Control. Daily transaction summary reports of the process will be forwarded from Production Control to the ILAM business owner. Resolution of problems encountered during the PMIS/ILAM process will be co-ordinated by Production Control, with assistance from personnel either from Notes Operations, PMIS operations, the ILAM developer or the ILAM business owner.

A log will be maintained for all approved LWOP leave transactions. The LWOP log is under development. The LWOP log will be used for archiving. It will also be used by HR Systems for ensuring the accuracy and completeness of processing from ILAM to the dedicated mailboxes, and processing by Pay and Benefits personnel.

Approved LWP requests will be archived in an Oracle database. Although the database structure has been developed, the interface is still under development. The LWOP logs will be archived after twelve months to a Lotus Notes database.

As at November 1, 1999 the pilot testing results (and evaluation sheets) had not been compiled or analysed. We have therefore not reviewed pilot results in detail. As at November 1, 1999, the ILAM team, although in the process of reviewing, have not yet signed off approval on the evaluation criteria that will migrate ILAM from Acceptance to Production.

FINDINGS

The following summarises the key findings of the review. Detailed observations and our assessment of the controls in ILAM are described in ***Appendix A***. Concerns or weakness noted in ***Appendix A*** are cross referenced to the applicable recommendation listed below.

Internal Controls

We reviewed internal controls by reviewing documentation, interviewing key project team members and by observing a demonstration of ILAM in NCR.

As part of internal control we have addressed the retention of back-ups and the ability to recover from failure. In addition, we have addressed internal controls over the data through five stages: data preparation; data input; data processing; data output; and data storage and disposal.

Back-ups and the ability to recover from failure

Notes databases, including ILAM databases, are routinely backed up by Notes Operations. PMIS is also routinely backed up in the course of PMIS operations. In addition, Production Control has implemented a procedure to update the PMIS leave module immediately prior to processing ILAM transactions.

Business continuity plans for Notes and PMIS are in place. A business continuity plan for ILAM has not been fully documented or finalised. The business continuity plan should include IT considerations, as well as user department alternative processing guidelines that would be required until the information services function restores service after a disaster or event. Considerations to include in the business continuity plan are detailed in **Appendix A** in the section, DS4: Ensure Continuous Service.

Other internal control issues are addressed within five stages:

1. Data Preparation

The implementation of ILAM will introduce improvements to data entry. Previously employees completed manual leave forms that were submitted to supervisors for approval. Approved requests were forwarded to Pay and Benefits and manually input to the PMIS leave module. Due to time constraints and workload, officers entering the data could not validate much of the information being entered. This resulted in data entry errors. With ILAM, employees enter their own leave requests directly into ILAM, immediately reviewing the accuracy of the data input. This is consistent with the fundamental principle of having data input conducted as close to the information source (employee) as possible. With ILAM, the information source is doing the data input.

2. Data Input

ILAM was designed to duplicate the paper form system, where employees and supervisors were responsible for ensuring the accuracy of the information (e.g., leave type, correct PRI, and correct dates). Once the data was entered, PMIS executed edit checks prior to processing (e.g., duration calculation, hourly/daily employee, leave entitlement).

Completeness and accuracy controls and some validation controls over the data exist in ILAM and PMIS[2]. However, validation of the legitimacy of the "supervisor" is not checked in ILAM or PMIS. This is a significant control weakness in that an employee's request (to add or delete) can be approved by someone without the appropriate authority to do so.

In the previous manual system, although Pay and Benefits personnel did not verify the signatures or names of supervisors, employees were required to present a written form to their supervisor for signature. At least three compensating controls were present in the manual system, but are not currently present in the ILAM based system. These three compensating controls, which discouraged and minimised the risk of processing illegitimately approved leave transactions were:

---

2 The accuracy of balances in ILAM will be partially dependent upon the accuracy of entitlements set up by the Pay and Benefits in PMIS. Immediately prior to the rollout of ILAM, the business owner has already identified the need to ensure all outstanding manual requests are entered into PMIS.

- Employees were required to obtain an actual signature, therefore requiring the employee to physically forge the signature or request someone else to illegitimately sign;
- Employees were aware that the leave request would be read and input by a Pay and Benefits Officer; and
- Employees were aware that Pay and Benefits would keep the piece of paper on hand.

In ILAM, an employee can assign any employee within Health Canada as his supervisor. The transaction is processed overnight in PMIS and updated the following day. Incentive and opportunity exists to submit an illegitimately authorized ILAM transaction because:

- the employee is no longer required to submit a physical piece of paper;
- the employee will be aware that a Pay and Benefits Officer will no longer be touching his leave form (at least not for LWP); and
- the employee could correctly assume that thousands of requests[3] will be processed through the ILAM, and may therefore view the likelihood of being caught as minimal.

Currently there are no compensating controls in ILAM or PMIS or the business process to minimise the risk, or detect occurrence, of processing illegitimately approved requests in ILAM and PMIS.

Table 1 below illustrates possible scenarios of processing illegitimately approved requests, notes the factors that currently exist that allow this scenario to occur, and lists examples of the types of compensating controls that could be considered. As with any internal control system, controls should manage the risk to a level acceptable to the organization. Therefore, the ILAM business owner must identify an acceptable risk level, and appropriate controls must be designed.

Table 1
Possible scenarios involving inappropriate authorization

Possible scenarios involving inappropriate authorization	Factors that enable scenario	Compensating controls to consider
SCENARIO ONE 1. Employee submits leave request to supervisor for legitimate vacation request of 10 days. 2. Employee assigns unauthorised "supervisor" (e.g. a colleague) to approve the deletion of that request, and approve a new request of 1 day vacation. 3. Employee is assigned to a new legitimate supervisor prior to year-end. 4. Employee reviews and approves year-end leave balance. 5. Employee receives cash out of the 9 unused	a) Employees can assign any other Health Canada employee as his "supervisor"; b) Legitimacy of supervisor is not verified in ILAM or PMIS; c) Employees may be unaware that ILAM records the identity of the originator and approver (and recommender) and that these records are kept on file; d) Supervisor #1 is not notified by ILAM that employee has changed supervisors; e) Human Resources has not developed review procedures to	a) Human Resources could ensure ILAM training highlights that ILAM records the identity of all transaction originators and all approvers, and that these logs are retained, and reviewed as a matter of routine management review b) Supervisors could receive e-mail notification that an employee has identified someone else as his supervisor for ILAM purposes, and then take action as required in each situation; c) Human Resources (possibly the ILAM project administrator) could

[3] The January 1998 Preliminary Project Impact Assessment for ILAM predicts annual volume of 157,850 transactions.

Possible scenarios involving inappropriate authorization	Factors that enable scenario	Compensating controls to consider
vacation days balance (despite having taken 10 days vacation).	identify unusual activity such as frequent supervisor changes or frequent delete activity related to LWP transactions; f) A supervisor is not notified by ILAM of the deletion of a previously approved transaction; g) A supervisor has access only to the employee's detailed transactions for which he/she acted as supervisor (although the supervisor does have access to the employee's net balances, such summary information may not easily highlight transaction activity); and h) Supervisors are not required to review and or sign off on employees' leave balances during the year-end review process.	receive e-mail notification that an employee has changed supervisors for ILAM purposes, and carry out some level of review on the reasonability of these changes; d) Authority to change supervisors could be limited to the existing supervisor and the employee's Pay and Benefits officer; e) Human Resources could carry out review procedures that randomly or statistically verify the appropriateness of supervisor changes and delete transactions; f) If "supervisor" #2 deletes a request approved by supervisor #1, supervisor #1 could receive e-mail notification of that delete so that the onus is on the supervisor to determine the requirement for any follow-up; and g) Human resources should ensure supervisors are fully aware of their responsibility to be familiar with and take responsibility for the accuracy/ reasonability of employees' leave transactions and balances.
SCENARIO TWO 1. Employee submits leave request to legitimate supervisor for a legitimate leave request of 10 days. (Assume this request would bring the employee's leave balance to zero.) 2. Employee assigns unauthorised "supervisor" (e.g. a colleague) to approve the deletion of original request, and approve a new leave request for only 2 days. 3. Employee is assigned a new supervisor. 4. Employee submits leave request for 8 days to the new supervisor, who is unaware that the employee's ILAM balance is actually short 8 days and should now be zero. 5. New supervisor approves leave request for 8 days. 6. Employee takes additional 8 days leave (all of which would be in excess of leave entitlement).	As above.	As above
SCENARIO THREE Same as above but for a leave request requiring two or more levels of approvals.	As above	As above

Possible scenario for flagging inappropriate authorization	Factors that enable scenario	Compensating controls to consider
SCENARIO FOUR 1. Employee submits leave request for 3 month Leave Without Pay (LWOP) to legitimate supervisor. 2. Employee assigns unauthorised "supervisor" (e.g. a colleague) to approve the deletion of that request, and approve a new request for 2 months LWOP. 3. Employee takes 3-month leave but payroll is only affected for 2 months.	As above plus: a) Pay and Benefits has not developed review procedures to identify unusual ILAM activity such as frequent supervisor changes or frequent delete activity related to LWOP transactions.	As above plus: a) Pay and Benefits could carry out review procedures that randomly or statistically verify the appropriateness of supervisor changes and delete transactions.

Controls exist over the processing of errors (LWP). PMIS will not process a transaction from ILAM that does not meet the data validation check in PMIS. However, there is a risk that errors will not be corrected and resubmitted in ILAM and ultimately into PMIS to update leave balances. Neither ILAM nor PMIS prompt or monitor the resubmission of corrected transactions. Since the employee has an incentive to not resubmit an erroneous transaction (keeping their leave balances high), the supervisor must be aware of the rejection, and of their responsibility to ensure rejected leave requests are corrected and resubmitted.

Controls over the processing of errors (LWOP) will be the responsibility of the Manager of Pay and Benefits. We are not aware of any business or review processes developed by or for Pay and Benefits that address:

a) validation or verification (especially validation of supervisors) of ILAM generated LWOP transactions; or
b) responsibilities for ensuring appropriate follow-up on rejected requests.

3. Data Processing

Some controls over data processing of ILAM transactions (LWP) are in place or in draft form, however, comprehensive and documented procedures to ensure the accuracy and completeness of processing, including action plans to resolve problems on a timely basis, are yet to be finalised.

The processing of LWP requests requires data processing procedures and controls for the following activities:

- the import of PMIS data;
- upload of ILAM data to PMIS;
- download from PMIS of erroneous transactions;
- audit trail into ILAM; and
- transfer of ILAM data to the Oracle archive database.

Similarly, the processing of LWOP requests requires data processing procedures and controls for the following activities:

- ensuring the accuracy and completeness of the generation of e-mails to the dedicated Pay and Benefits mailboxes for approved transactions;
- ensuring the accuracy and completeness of audit trail or log into ILAM; and
- the transfer of ILAM data to the Notes archive database.

4. Data Output

Controls over output are in place, although some procedures are yet to be finalised such as the daily review of the ILAM error and audit trail log by the ILAM business owner.

Employees can print their own ILAM information and safeguard as considered necessary by each employee. Supervisors also can print an employee's ILAM summary and transaction details for ones which they acted as supervisor. Supervisors should be aware of the privacy considerations of handling such output.

Access to leave transaction and balance information is controlled. Until recently, leave summary reports from PMIS were provided annually to employees for review and sign-off.

Recently Health Canada decided that as an alternative to the annual employee sign-off, employees will be required to notify Pay and Benefits within 10 days of any disputed leave transactions or balances. If Pay and Benefits are not notified within 10 days, the transactions will be deemed accepted by the employee. Leave Summary reports from PMIS will continue to be provided annually for review to those employees who do not have access to ILAM.[4].

5. Data Storage and Disposal

Existing data storage and disposal procedures are in place to manage ILAM data.

LWP transactions will be archived in the Oracle database, and will be managed by Production Control. LWOP transactions will be archived in a Notes database managed by Notes Operations. Procedures to manage and control the archiving activities are not yet finalised.

---

[4] Such a policy requires careful consideration. For example, employees could easily be away on leave for more than 10 days. Also, if the employee has only 10 days to correct an error, consideration should be given to whether the employer will be limited to the same 10 day window to correct ILAM or PMIS errors (clerical, fraudulent or otherwise).

Recommendations

Recommendation topic	*It is recommended that:*
1) Business Continuity and User Department Alternative Processing Back-up Procedures	Human Resources should: a) ensure that Production Control has developed and approved ILAM continuity plans that meet Human Resources business requirements; and b) develop and approve alternative-processing procedures (LWP and LWOP) that may be used in the event ILAM service is disrupted.
2) Validation of Supervisors	Human Resources, being the ILAM business owners, should address the need to design and implement controls (preventative and detective) to ensure the validity of supervisors assigned to approve ILAM transactions. The level of controls must manage the risk to a level acceptable to Human Resources. Possible alternatives are presented in **Table 1**.
3) Review Procedures (LWP and LWOP)	a) Human Resources should develop and formalise review procedures based upon Health Canada's accepted risk level, that ensure the integrity of ILAM transactions (LWP) processed by PMIS. b) Pay and Benefits should develop and formalise review procedures, based upon Health Canada's accepted risk level, that ensure the integrity of ILAM transactions (LWOP) processed by Pay and Benefits personnel.
4) Processing Control Procedures (LWP, LWOP and Oracle archiving)	a) Production Control should finish development of all ILAM - related control requirements (including action plans to resolve problems) that ensure accuracy and completeness of processing. These procedures should be fully documented and approved by Production Control management. b) Human Resources should develop and approve control processes required to ensure the accuracy and completeness of the receipt of e-mails in the Pay and Benefits mailboxes of approved ILAM requests (LWOP). c) Production Control, once formally assigned the responsibility by Human Resources, should develop, document and approve procedures to control and monitor the transfer of ILAM transactions to the Oracle archive database. d) Human Resources should assign responsibility for archiving LWOP logs and ensure processing requirements are documented and finalized by the responsible party.
5) Privacy and supervisor privacy considerations	Human Resources should ensure ILAM training addresses privacy issues regarding the safeguarding by supervisors of any ILAM printouts of employee information.
6) Error handling	Human Resources, being the ILAM business owner, should formally assign responsibility, and develop processes, for following up on: a) ILAM transactions rejected by PMIS; b) ILAM transactions rejected by Pay and Benefits; c) ILAM leave requests not acted upon by supervisors; and d) ILAM mail messages that are undeliverable.

Security

Security controls are dictated, in part, by the sensitivity of the data through formal data classification. ILAM data has been classified as Protected B, the same classification as PMIS information.

There are controls in place to restrict unauthorised access to ILAM information. Access to ILAM is via an employee's Lotus Notes password, subject to the Notes identification, authentication and access controls already in place, managed by the Lotus Notes Operations group. These controls could however, be compromised by the employee's failure to safeguard his password or to utilise the F5 function that requires re-entry of Notes password should the employee be away from his computer screen.

Although the ILAM business owner has formally communicated ILAM access profiles to Notes Operations for the pilot, final ILAM access profiles have not been communicated. These profiles should include access requirements (regional and NCR) for Notes Operations, Production Control, Human Resources, and Pay and Benefits.

Each employee is restricted to accessing his own ILAM information. Supervisors can access ILAM information for employees for which they have been assigned "supervisor". Such access is limited to viewing the employee's balance, viewing details of transactions for which they acted as supervisor, and initiating requests on behalf of the employee. In instances when the supervisor initiates a request on behalf of the employee, the employee is automatically notified by an ILAM generated e-mail.

Access to the PMIS leave module is managed by the PMIS security officer. Currently, access includes Pay and Benefits personnel, Production Control personnel, and miscellaneous personnel in regions (due to workload pressures on Pay and benefits personnel), and in NCR (e.g. Policy and Advisory Services Division, Medical Services Branch, Corporate Services Branch & Executive Offices). Prior to the roll out of ILAM, and on an ongoing basis, the appropriateness and necessity of access to the PMIS leave module should be reviewed, with consideration given to ILAM implications.

Notes has the capacity to monitor certain security and other violations within Notes databases such as ILAM. Production Control and HR Systems will be responsible for monitoring these activities. To date, the triggers or flags to be monitored have not been identified. Examples of activities to be monitored could include instances where a user has tried to log on to Notes with say, four erroneous password attempts, or when a user has tried repeatedly to approve his own transaction.

Recommendations

Recommendation topic	*It is recommended that:*
Note: In a November 17, 1999, phone discussion, the ILAM business owner noted recommendations, 7 to 10 were addressed subsequent to issuance of the draft report. We have not reviewed the documentation to support these subsequent actions and therefore cannot comment on their completeness or effectiveness.	
7) Notes security considerations	Human Resources should ensure ILAM training highlights the importance of security precautions users should take regarding access to their Notes and ILAM databases.
8) PMIS leave module access	Human Resources should ensure PMIS leave module access rights are updated to reflect ILAM security considerations.
9) Oracle and LWOP log rights	Human Resources should finalise access rights for the Oracle database and the LWOP log.
10) ILAM access rights	Human Resources should finalise (and formally communicate to Notes Operations) ILAM access rights for LAN personnel, Notes Operations personnel (NCR and regional), Production Control personnel and any other specialised access rights. Such access rights should be reviewed by the ILAM business owner on an as required basis.
11) Monitoring by Security and Other Violations	Production Control and HR Systems should finalise the processes for monitoring and reporting on specific ILAM security or other violations as well as on certain Notes security violations, that may impact upon the security of ILAM.

CobiT Processes and Objectives
And
Observations and Assessment

The following table describes our observations and assessment of the controls in ILAM. With respect to reviewing the accuracy of the PMIS/ILAM interface, we completed several ILAM transactions during the demo in NCR, and on the following day, reviewed the PMIS/ILAM processing logs, PMIS screens, and the updated ILAM summaries. We checked to ensure our sample transactions were processed (or not processed, if the transaction was for the next fiscal period or if it was rejected by PMIS) in PMIS. Although, as at November 1, 1999, the pilot testing results had not been received, analysed and reviewed by the ILAM Project Team, we were able to review the summary results the ILAM Project team's detailed testing of ILAM/PMIS updating done over a three day period from October 18 to 29, 1999 (approximately 270 transactions) The interface to the Oracle database is not yet in place, and therefore we were not able to observe any of the controls surrounding the transfer of records from ILAM to Oracle. The LWOP audit log is currently under development and we were therefore not able to review the accuracy, completeness or usefulness of the log.

The audit addressed only application security and not the security over the infrastructure such as the network, operating system, physical and telecommunications.
The following observations and assessment of the controls are based upon:

- Interviews and discussions with the following individuals;

David Windsor	Production Control (re: Oracle database)
Lizabeth Gray	Asst to ILAM Project Leader
John Campeau	Notes Operations
Darquise Gauthier	ILAM developer
Joanne Chartrand	PMIS Security Officer
Donald Constantineau	Production Control
Sylvie Bouillon	PMIS Project Leader
Pauline Thériault	ILAM Project Leader

- A demonstration of ILAM on October 8, 1999, by Pauline Thériault; and
- Review of
  - various documentation, logs, reports and memos provided by the interviewees;
  - various documentation, test results, memos, reports and logs included in the ILAM Workbook, Training Database, Help Database, and Acceptance Testing Log; and
  - previous audit report, working papers and ILAM team response to the audit recommendations.

Recommendations

Recommendation topic	*It is recommended that:*
Note: In a November 17, 1999, phone discussion, the ILAM business owner noted recommendations, 7 to 10 were addressed subsequent to issuance of the draft report. We have not reviewed the documentation to support these subsequent actions and therefore cannot comment on their completeness or effectiveness.	
7) Notes security considerations	Human Resources should ensure ILAM training highlights the importance of security precautions users should take regarding access to their Notes and ILAM databases.
8) PMIS leave module access	Human Resources should ensure PMIS leave module access rights are updated to reflect ILAM security considerations.
9) Oracle and LWOP log rights	Human Resources should finalise access rights for the Oracle database and the LWOP log.
10) ILAM access rights	Human Resources should finalise (and formally communicate to Notes Operations) ILAM access rights for LAN personnel, Notes Operations personnel (NCR and regional), Production Control personnel and any other specialised access rights. Such access rights should be reviewed by the ILAM business owner on an as required basis.
11) Monitoring by Security and Other Violations	Production Control and HR Systems should finalise the processes for monitoring and reporting on specific ILAM security or other violations as well as on certain Notes security violations, that may impact upon the security of ILAM.

CobiT Processes and Objectives And Observations and Assessment

The following table describes our observations and assessment of the controls in ILAM. With respect to reviewing the accuracy of the PMIS/ILAM interface, we completed several ILAM transactions during the demo in NCR, and on the following day, reviewed the PMIS/ILAM processing logs, PMIS screens, and the updated ILAM summaries. We checked to ensure our sample transactions were processed (or not processed, if the transaction was for the next fiscal period or if it was rejected by PMIS) in PMIS. Although, as at November 1, 1999, the pilot testing results had not been received, analysed and reviewed by the ILAM Project Team, we were able to review the summary results the ILAM Project team's detailed testing of ILAM/PMIS updating done over a three day period from October 18 to 29, 1999 (approximately 270 transactions) The interface to the Oracle database is not yet in place, and therefore we were not able to observe any of the controls surrounding the transfer of records from ILAM to Oracle. The LWOP audit log is currently under development and we were therefore not able to review the accuracy, completeness or usefulness of the log.

The audit addressed only application security and not the security over the infrastructure such as the network, operating system, physical and telecommunications.
The following observations and assessment of the controls are based upon:

- Interviews and discussions with the following individuals;

David Windsor	Production Control (re: Oracle database)
Lizabeth Gray	Asst to ILAM Project Leader
John Campeau	Notes Operations
Darquise Gauthier	ILAM developer
Joanne Chartrand	PMIS Security Officer
Donald Constantineau	Production Control
Sylvie Bouillon	PMIS Project Leader
Pauline Thériault	ILAM Project Leader

- A demonstration of ILAM on October 8, 1999, by Pauline Thériault; and
- Review of
  - various documentation, logs, reports and memos provided by the interviewees;
  - various documentation, test results, memos, reports and logs included in the ILAM Workbook, Training Database, Help Database, and Acceptance Testing Log; and
  - previous audit report, working papers and ILAM team response to the audit recommendations.

CobiT Processes and Objectives And Observations and Assessment

CobiT Process Area	Control Objectives	Observation	Our Assessment
DS4 Delivery & Support: Ensure Continuous Service			
4.3 Information Technology Continuity Plan Contents	Information services function management should ensure that a written plan is developed containing the following: • identification of the critical application programmes, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs. • Guidelines on how to use the continuity plan; • Response procedures meant to bring the business back to the state it was in before the incident or disaster; • Recovery procedures meant to bring the business back to the state it was in before the incident or disaster; • Procedures to safeguard and reconstruct the home site; • Communication procedures with stakeholders including employees, and management; • identification of alternatives regarding the back-up site and hardware as well as a final alternative selection. If applicable, a formal contract for these type of services should be concluded; and • Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media. Information services function management should establish procedures and guidelines for minimizing the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture.	• Continuity plans exist for Notes and PMIS leave module • Notes databases in NCR are completely backed up by Notes Operations on a daily, weekly and monthly basis. Daily files are kept for 8 weeks, weekly and monthly tapes are kept indefinitely. • Responsibility for Notes back-up in the region rests with regional Notes Operations and is detailed in the Sept 99 version of ILAM Roles and Responsibilities *(This document was apparently finalised on November 4, 1999)*—note that back-up of regional Notes servers may be a non-issue if replication approach is no longer valid • PMIS is backed up immediately prior to PMIS/ILAM processing, this is in addition to routine PMIS back-up processes • Continuity plan for ILAM module has not yet been developed documented and approved.	A Business Continuity Plan for ILAM has not been developed, documented and approved. ***(See Rec. 1)***

CobiT Processes and Objectives And Observations and Assessment

CobiT Process	Control Objective	Observation	Risk Assessment
4.5 Maintaining the Information Technology Continuity Plan	Information services function management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resources procedures. Information services function management should establish "wrap-up" procedures, invoked on successful resumption of the information services function after a disaster, for assessing the adequacy of the plan and update the plan accordingly.	ILAM continuity plan not yet developed, specific change control procedures not yet addressed.	*(See Rec. 1)*

CobiT Processes and Objectives And Observations and Assessment

4.6 Training for and Testing the Information Technology Continuity Plan	The disaster continuity methodology should ensure that all concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster. To have an effective continuity plan, management needs to assess its adequacy on a regular basis; this requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.	ILAM continuity plan not yet developed therefore training and testing requirements not defined.	*(See Rec. 1)*
4.8 Information Technology Continuity Plan Distribution	Given the sensitive nature of information in the continuity plan, the latter should be distributed only to authorised personnel and should be safeguarded against unauthorised disclosure. Consequently, sections of the plan need to be distributed on a need - to - know basis.	Distribution limitations for continuity plan not yet defined.	*(See Rec. 1)*
4.9 User Department Alternative Processing Back-up Procedures	The continuity methodology should ensure that the user departments establish alternative-processing procedures that may be used until the information services function is able to fully restore its services after a disaster or event.	In the event that ILAM is not operational, employees would be required to revert to manual processes. Human Resources has not yet documented for all stakeholders (i.e. employees, supervisors, Pay & Benefits, etc.) the requirements for, and implications of, reverting to a manual process.	Not yet addressed. *(See Rec. 1)*

CobiT Processes and Objectives
And
Observations and Assessment

CobiT Process Area	Control Objectives	Observation	Our Assessment
DS4 Delivery & Support: Ensure Systems Security			
5.2 Identification, Authentication and Access	The logical access to and use of the information services function's computing resources should be restricted by the implementation of an adequate authentication mechanism of identified users and resources associated with access rules. Such mechanisms should prevent unauthorized: • personnel; • dial-up connections; and • other system (network) entry ports, From accessing computer resources. Such mechanisms should also minimise the need for authorised users to use multiple sign -ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).	**ILAM:** --accessible to all departmental employees with a Notes Profile through a default profile for all departmental employees. --first time entry to ILAM is controlled through input of the employee's notes password, the employee's PRI and birthdate (PRI and birthdate is validated against the information stored in ILAM from PMIS) --subsequent entry to ILAM requires only input of the employees notes password --only employee and assigned supervisors have access to employee's information --ILAM password control exists through Lotus Notes --attempts to gain access to Lotus Notes does not result in revocation of access rights, however, repeated erroneous password attempts does result in a progressively slower response from Notes for access—once correct password is entered response time reverts to normal --although Notes Operations keeps a log of repeated entry attempts this log is reviewed only upon request --ILAM training should highlight the need for employees to consistently use the F5 key to block access to Lotus Notes (and therefore to ILAM) --through Notes, ILAM has dial-in capabilities --no other applications can be accessed through ILAM—ILAM transactions are uploaded to PMIS in an offline batch process **PMIS:** --Access rights are controlled by Joanne Chartrand—rigorous passwords and access controls exist within PMIS, preventing unauthorised access --Currently several non HR employees (primarily in the regions) have access to PMIS to change leave data --selected programmers have dial-in access --PMIS has a firewall	There is a risk that unauthorised persons could obtain access to an employee's ILAM information. . ***(See Rec. 7 and 10)*** There is a risk that unauthorised persons could change ILAM transactions in PMIS. ***(See Rec. 8)***

CobiT Processes and Objectives And Observations and Assessment

CobiT Process	Control Objective	Observation	Our Assessment
5.3 Security of Online Access to Data	In an online information technology environment, information services function's management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.	--ILAM security profiles have been established for the pilot, access has been set up for users, Notes server administrators, production control —final security profiles (NCR and Regional) to be used when ILAM is in production have not been approved and finalised by the client, nor have they been communicated to Notes Operations for establishing access to ILAM through Notes *(Subsequent to completion of the field work for this audit, we understand these profiles have apparently been finalised.)* --access to ILAM files is dependent upon initial entry of valid PRI and birthdate, access thereafter is limited to user and assigned supervisors --however, there is no validation of whether the approver of the leave request is the bona fide supervisor of that employee;	ILAM security profiles for all groups need to be finalised and communicated to Notes Operations. ***(See Rec. 10)*** A risk exists that an ILAM leave request can be created or deleted by an unauthorised supervisor. . ***(See Rec. 2)***
5.4 User Account Management and Management Review of User Accounts	Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. Management should have a control process in place to review and confirm access rights periodically.	Joanne Chartrand manages PMIS user access, periodic reviews of user access rights are carried out --Notes ID manages the granting of password/access privileges for all Lotus Notes applications, as directed by change requests through the Help Desk— --ILAM access rights are required by NCR Notes Operations personnel, some regional Notes Operations personnel, and Pay and Benefits personnel, by pay list. The necessity and appropriateness of these access rights should be reviewed by ILAM business owner on a periodic basis. *(Such a process was not yet in place as at the end of our field work. We understand that such processes have now apparently been finalized.)* --ILAM access to users is restricted to their own leave information. There is no need to review this generic access for each user.	Process is in place to manage PMIS access, but such process should consider ILAM implications. ***(See Rec. 8)*** ILAM access should be formally finalised and communicated to Notes Operations. . ***(See Rec. 10)***
5.6 User Control of User Accounts	Users should systematically control the activity of their proper account(s). Also information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.	Each employee can view his or her activity on a daily basis. In addition: • employees are immediately notified of requests rejected by supervisors; • employees and supervisors are notified of any PMIS processing errors on the following day; • employees are notified of any leave requests submitted on their behalf by a supervisor; and • each employee is required to bring any discrepancies to the attention of Pay and Benefits, within 10 days of the transaction.	Users can review and control their ILAM activity, but such review and control is limited by a recent Health Canada policy decision that requires employees to notify Pay and Benefits of any discrepancies within 10 days ***(see Page 9)***

CobiT Processes and Objectives And Observations and Assessment

CobiT Process	Control Objective	Observation	Risk Assessment
5.7 Security Surveillance	The information services function's security administration should ensure that security activity is logged and any indication of imminent security violation is notified immediately to the administrator and is acted upon automatically.	• Attempts to log-in to Notes are logged by Notes Operation. The list of log attempts is available for review, if requested. • Notes Operations has the capacity to identify log in attempts and other "violations" (e.g. attempts to perform a function for which user does not have authority) within Notes applications. Such violations will be reviewed by Production Control and HR Systems. • ILAM has not identified monitoring or threshold requirements related to log-in attempts and ILAM-specific "violation" instances • The practicality or feasibility of such monitoring requirements has not been addressed.	ILAM business owner has not formalised security surveillance requirements. ***(See Rec. 11)***.
5.8 Data Classification	Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated	ILAM data has been classified as Protected B information, which is the same classification as PMIS data.	Data has been classified as Protected B and as such access to ILAM data is restricted to the employee and supervisor.
5.9 Central Identification and Access Rights Management	Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.	Lotus Notes password allows access only to ILAM. The upload of ILAM to PMIS is an off-line batch run each evening. PMIS access is controlled and monitored.	Access to ILAM does not allow access to other applications.
5.10 Violation and Security Activity Reports and Incident Handling	The information services function's security administration should assure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorised activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know. Management should establish a computer security incident handling capability to address security incidents by providing a centralised platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.	See 5.7	See 5.7
5.12 Re-Accreditation	Management should ensure that re-accreditation is periodically performed to keep up-to-date the formally approved security level and the acceptance of residual risk.	See 5.7	See 5.7

CobiT Processes and Objectives And Observations and Assessment

[illegible]	[illegible]	[illegible]	[illegible]
5.15 Non-Repudiation	Organisational policy should ensure that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions.	• originator and supervisor recorded in each ILAM transaction, recorded in audit trails, retained as part of ILAM back-ups kept indefinitely by Notes Operations, as well as kept in Oracle archive for seven years • possibility exists that users could deny input or approval of a transaction, claiming another user had accessed their Notes, and therefore, their ILAM information—risk is low because such claims could be repudiated by departmental policy to keep Notes passwords confidential, periodically change Notes passwords, use F5 key to deny access to Notes when employee leaves desk, and instruction to employees to periodically review their ILAM transactions and balances and report discrepancies to Compensation & Benefits	The risk that users can deny transactions should be minimised. (***See Rec. 7***).

CobiT Processes and Objectives
And
Observations and Assessment

[illegible]	[illegible]	[illegible]	[illegible]
DS10 Delivery & Service: Manage Problems and Incidents			
10.1 Problem Management System, Problem Escalation, and Audit Trail	Information services function management should define and implement a problem management system to ensure: • that all operational events which are not part of the standard operation (incidents, problems and errors) are recorded, analysed and resolved in a timely manner. Incident reports should be established in the case of significant problems.; and • that identified problems are solved in the most efficient way on a timely basis. These procedures should ensure that these priorities are appropriately set. The procedures should also document the escalation process for the activation of the information technology continuity plan. • The problem management system should provide for adequate audit trail facilities which allow tracing from incident to underlying cause (e.g., package release or urgent change implementation) and back. It should closely interwork with change management, availability management and configuration management.	**LWP** • Nightly PMIS/ILAM off-line process is managed by Production Control • Draft processes for dealing with any PMIS/ILAM processing problems are detailed in Roles and Responsibilities of Technical Support • Detailed procedures for resolving operational problems during the PMIS/ILAM processing are not fully documented, approved or finalised **LWOP** • The ILAM business owner will be responsible for ensuring all approved LWOP requests in ILAM triggers a message to Pay and Benefits, this process has not been developed, nor have processes to resolve problems—*(Based on discussions with the ILAM business owner we understand these processes are considered necessary and therefore will not be developed).*	Operational events (related to LWP and ILAM. PMIS processing) that are not part of the standard operation are recorded and timetable by Production Operations. However, procedures for analysing and resolving these problems, although in draft form, have not been fully documented, nor have they been formally approved by Production Control management. ***(See Rec. 4)*** A problem management system to address processing of LWOP transactions has not yet been addressed. ***(See Rec. 4)***

CobiT Processes and Objectives
And
Observations and Assessment

[illegible]	[illegible]	[illegible]	[illegible]
DS11 Delivery & Service: Manage Data			
11.1 Data Preparation Procedures	Data preparation procedures and controls should be established, including: • Input form design to minimise errors and omissions; • Source document authorisation, including adequate segregation of duties; • Source document collection procedures to ensure completeness and accuracy; • Error handling procedures; • Definition of source document retention requirements	--Data is input directly into ILAM by the employee, there is no input form, and ILAM checks for various logistics including stop/start dates for term employees ----the employee has the opportunity to review the accuracy of the data prior to submitting it for approval to his/her supervisor --in certain instances, a supervisor may input leave request for the employee—the supervisor has the opportunity to review the information for accuracy prior to submitting it to a third party for approval and the employee will have the opportunity to review the accuracy of the transaction upon receipt of an e-mail regarding the transaction submitted on his/her behalf --the likelihood of date errors is minimised because the employee selects dates from a calendar --source document collection procedures to ensure completeness: processes to ensure transactions rejected by PMIS or transactions that sit unapproved in ILAM are followed up appropriately have not been finalized –although supervisors and employees are forwarded reminder e-mails of unapproved requests waiting in ILAM, responsibility to ensure appropriate follow-up action is taken has not been formally assigned. ---source document retention requirements—see 11.19	Data preparation controls have improved with input directly from the source. There is a risk that transactions will be approved by unauthorised persons. ***(See Rec. 2)*** Error handling procedures have not been finalised. ***(See Rec. 6)***

CobiT Processes and Objectives And Observations and Assessment

CobiT Process No.	Control Objective	Observation	Risk Assessment
11.2 Data Input: Authorisation	Data input procedures and controls should be established, including: • Data input should be performed only by authorised staff	***Authorisations*** data input controls noted: --each employee is authorised to enter leave data into ILAM, transactions cannot be authorised by the requesting employee --employees can access only their own ILAM account --supervisors can access only their own ILAM account, and only for those employees for whom they have been assigned supervisor --if a supervisor inputs a leave request on account of an assigned employee, the employee is notified of the request via Notes, and can take appropriate action as required (i.e. Contact supervisor, Pay and Benefits, etc.) --transactions cannot be authorised by a supervisor inputting a request on behalf of an assigned employee—third party authorisation is required --attempts to submit leave requests in excess of leave balances are not accepted --user can access ILAM profile only for employees for whom the user is assigned as supervisor (i.e. a user cannot access ILAM data for another employee even if he/she knows the other employee's PRI and birthdate) --ILAM records in the workflow, the identity of the originator, the recommender and the approver --data input control weaknesses: --approval of data input could be done by unauthorised supervisors, since there are no controls in ILAM or PMIS --a risk exists that unauthorised persons could access an employee's or supervisors Notes databases, including ILAM	A risk exists that non-authorized users could access an employee's or supervisor's Notes (and therefore ILAM) account. ***(See Rec. 7)*** Supervisors are not validated in ILAM or PMIS (*See Rec. 2)*

CobiT Processes and Objectives And Observations and Assessment

CobiT Process	Control Objective	Observation	Risk Assessment
11.7 Data Input: Accuracy, Completeness and Validity	Data input procedures and controls should be established, including: • Transaction data entered for processing (people generated, system-generated or interfaced inputs) is subject to a variety of controls to check for accuracy, completeness and validity	Data input controls noted: ---PMIS validation controls have already been established and continue to operate (including existence, completeness and or accuracy checks on transaction type, fiscal year, PRI, pay office, leave month, leave code, start date, end date, employment period, duration flag—hours or days, variable work week versus normal work week, addition to leave summary, delete from leave summary) --ILAM carries out several validation edits of data entered (including validation of date, PRI, birthdate, leave code, compressed work week, transaction type, duration calculation, leave balances) --ILAM prompts user for sick certificates in accordance with contract requirements, responsibility to follow up on receipt of certificates rests with the supervisor, as in the manual process --ILAM calculates duration of leave --ILAM notifies employee that approved LWOP request has been forwarded to Pay & Benefits --PMIS carries out most of the validity checks as previously noted—PMIS validation includes checking for duplicate leave requests -Pay and Benefits will be instructed to ensure all leave balances are up to date prior to start of roll-out Data input weaknesses noted: ----no validation of approver or recommender—employee can assign any other employee as supervisor --although the name of any unauthorised "supervisor" would be recorded in the leave workflow, this information would only be available to the employee—it would not be visible to the legitimate supervisor because the supervisor has access only to those transactions for which he was assigned supervisor --a request approved by supervisor #1 can be deleted by supervisor #2 (without any notice to supervisor #1)	Data input controls to check for accuracy and completeness of data input are adequate. Data input controls to check for validity of the approver are not adequate. ***(See Rec 2).***
11.8 Data Input: Error Handling	Data input procedures and controls should be established, including: • Correction and resubmission of data that was erroneously input	--if PMIS rejects an erroneous transaction (that has been approved by the supervisor in ILAM), the originator receives an error message the next day explaining the error --responsibility to follow-up on correction of the PMIS-rejected transaction (that has bren approved in ILAM) has been identified as a responsibility of the employee --responsibility to ensure a corrected leave transaction is input, approved and recorded to reflect any actual leave taken should rest with the supervisor (employee has no incentive to re-submit) --rejected transactions are deleted from ILAM after 20 days --the approving supervisor will only be aware of the rejected transaction if he/she reviews the employee's leave records within 20 days of the rejection and notices the status of the specific transaction , this is unlikely	Procedures and controls to correct and re-submit erroneous input have not been finalised. ***(See Rec. 6)***

CobiT Processes and Objectives And Observations and Assessment

CobiT Process	Control Objective	Observation	Risk Assessment
11.9 Data Processing: Integrity and Validation and Editing	Data processing controls should be defined, including: • Separation of duties is maintained; and • Adequate update controls such as run-to-run control totals and master file update controls are in place; and • Validation, authentication and editing are performed as close to the point of origin as possible.	**LWP:** • Processing is maintained separate from data input—ILAM transactions processed in offline batch, managed by Production Control • Production Control has developed preliminary processes for daily review and analysis of review of nightly cycle (including export of ILAM data, receipt by PMIS, processing by PMIS, and subsequent update of ILAM)—*(Although these processes had not been documented or finalised as at the end of our field work, we understand they have since been completed.)* • Processes are required to address requirements for processing and problem resolution related to the import of PMIS data, the upload of ILAM data to PMIS, the download from PMIS of erroneous transactions an audit trails into ILAM **LWOP:** • Processing is maintained separate from data input—requests input by employee and approved by supervisor, approved request processed by Pay and Benefits • Access to the Pay and Benefits mailbox is limited as follows: Managers, have update access, other Compensation and Benefit, have read access. • ILAM business owner has not finalised processes for daily review of the accuracy and completeness of e-mails forwarded to the Pay and Benefits mailboxes • Review procedures to be carried out by Pay and Benefits, although in process, have not been finalised **Note:** Prior to roll-out of ILAM, the business owner has established a process to ensure PMIS leave balances are current.	Data processing controls for PMIS/ILAM processing (LWP) although drafted for the most part, have not been fully documented, nor approved. ***(See Rec. 4)*** Data processing controls for processing of LWOP have not been developed, documented, nor approved. ***(See Rec. 4)*** Review procedures to be carried out by Pay and Benefits, although in process, have not been finalised. ***(See Rec. 3)***

CobiT Processes and Objectives
And
Observations and Assessment

[illegible]	[illegible]	Observation	[illegible]

11.11 Data Processing: Error handling	Data processing controls should be defined, including:
	• Error handling procedures that enable erroneous transactions to be identified without being processed and without undue disruption of the processing of other valid transactions.
		LWP
		• Approved LWP requests are processed as part of the PMIS/ILAM batch cycle, requests not approved in ILAM remain in ILAM for 20 days, after which they are deleted—the unapproved requests do not affect the timely processing of unapproved requests
		• Approved ILAM requests that are rejected by PMIS are not processed by PMIS, they are recorded in the audit trail, and an e-mail message is forwarded to the originator of the rejected request
		• PMIS numeric error messages have been translated into practical error messages that will be sent to employees for follow-up *(Final review and approval of these error messages to ensure appropriate information is provided to the employee and to Pay and Benefits had not been finalised as at the end of our field work. We understand it has subsequently been completed.)*
		  • A process to ensure all error messages are acted upon has not been developed, nor has responsibility been designated
		  • A process to ensure all unapproved requests are appropriately followed up has not been addressed
		LWOP
		• Upon receipt of the ILAM generated e-mail, approved LWOP requests are processed by Pay and Benefits
		• Unapproved requests remain in ILAM for 20 days, after which they are deleted—the unapproved requests do not affect the timely processing of unapproved requests
		• A process to ensure all unapproved requests are appropriately followed up, although in development, is not finalized
			Error handling processing controls have not been fully documented or approved. ***(See Rec. 6)***

CobiT Processes and Objectives
And
Observations and Assessment

CobiT Process Area	Control Objective	Observation	Our Assessment
11.12 Output Distribution: Handling, security and retention, distribution, balancing, output review and error handling	Data output procedures and controls should be defined, including: • Distribution and security of output, including hard copy and electronic distribution; • Audit trails and procedures to ensure that output routinely is balanced to the relevant totals; and • Accuracy of output is reviewed, including procedures for controlling errors contained in the output	Distribution and security of output • Employees can print and safeguard own information as considered necessary • Supervisors can print and review employee's transactions and leave balances—managers should be made aware of safeguarding and privacy issues of such information • Pay and Benefits personnel can print and review ILAM or PMIS information—Pay and Benefits fully aware of privacy requirements of such personnel information Audit trails and procedures to balance—process control 4 **LWP** • Production Control uses audit trails to ensure output from PMIS is balanced to ILAM transactions input, these procedures are not finalized. **LWOP** • The LWOP audit log has not yet been finalized nor have processes to balance ILAM transactions to e-mails received in the Pay and Benefits mailbox. (Note: these processes will likely be the responsibility of the soon to be hired ILAM Project Administrator. Review of output including procedures for controlling errors—see 2.2	Data output guidelines for supervisors that address privacy issues and review requirements should be addressed. ***(See Rec. 5)*** Production Control processing procedures need to be finalized ***(See Rec. 4)*** Procedures to ensure the completeness of ILAM transactions (LWOP) received by Pay and Benefits need to be finalized. ***(See Rec. 4)***
11.19 Storage Management	Procedures should be developed for data storage, which consider retrieval requirements, and cost effectiveness and security policy.	• ILAM transactions will be downloaded to Oracle database when the following criteria are met: the transaction is over 12 months old, the transaction was approved, the transaction was accepted by PMIS • Oracle database records will be maintained for seven years • Procedures to manage and control access to the Oracle archived information, although in process, are not finalised • Details of LWOP transactions approved in ILAM will be stored in the LWOP logs, this log is currently under development • Procedures to manage and control access to the LWOP logs, although in process, are not finalised *(We understand that only Pay and Benefits, and the ILAM Administrative group will have access to the LWOP log)* • LWOP logs will be kept for one year, then archived in a Lotus Notes database and kept for seven years	Procedures for data storage related to the Oracle archiving and LWOP logs should be finalised. ***(See Rec. 9).***

CobiT Processes and Objectives And Observations and Assessment

[illegible]	[illegible]	Observation	[illegible]
11.23 Back-up and Restoration	Management should implement a proper strategy for back up and restoration to ensure that it includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan. Procedures should be set up to ensure that back-ups are satisfying the above-mentioned requirements. Procedures should be in place to ensure back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.	See 4.3	See 4.3
11.24 Back-up Jobs	Procedures should be in place to ensure back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.	See 4.3	See 4.3
11.26 Archiving	Management should implement a policy and procedures for ensuring that archival meets legal and business requirements, and is properly safeguarded and accounted for.	See 11.19	See 11.19

CobiT Processes and Objectives
And
Observations and Assessment

M2 Assess Internal Control Adequacy				

2.2	Timely Operation of Internal Controls	Reliance on internal controls requires that controls operate promptly to highlight errors and inconsistencies, and that these are corrected before they impact production and delivery. Information regarding errors, inconsistencies and exceptions should be kept and systematically reported to management.	• Procedures are not defined for the reporting of errors, inconsistencies and exceptions to management.
			
			LWP:
			• During the pilot, Production Control provided HR with a daily summary of ILAM transactions (used by HR to monitor pilot volume)
			• A format for such a report after the roll-out has not been finalised
			• A more detailed version of the audit trail was developed by Production Control and provided to the ILAM application owner for review (volume only) during the pilot
			  • Initial version did not include name of approver.--subsequent draft versions have.
			  • Format, content and "readability" requirements of the daily LWP audit trail need to be addressed by ILAM business owner, and developed by Production Contro'
			• Such a report should highlight or flag "Unusual" (i.e. suspicious or otherwise) ILAM transactions
			  • Examples of the type of information such a report could highlight for HR would be, for example, # of delete transactions, # of rejected transactions, # of instances where the supervisor has changed more than three times in the last month (or some similar criteria)
			• Such a report from Production Control could be used by the ILAM business owner (likely the soon to be hired ILAM Project Administrator) to carry out internal control review-
			• Examples of the type of information such a report could highlight for HR would be, for example, # of delete transactions, # of rejected transactions, # of instances where the supervisor has changed more than three times in the last month (or some similar criteria)
				There is a risk that a systematic error or control failure may not be brought to the attention of senior management. ***(See Rec. 2)***

CobiT Processes and Objectives
And
Observations and Assessment

[illegible]	[illegible]	[illegible]	[illegible]

2.2 Timely Operation of Internal Controls (cont'd)		**LWOP**
		• Pay and Benefits personnel will be responsible for developing processes for reviewing approved LWOP requests—these procedures have not been finalized
		• An audit trail report (LWOP transactions) is in the process of being developed
		• Access to this LWOP log will be limited to the ILAM business owner and Pay and Compensation managers
		  • The ILAM business owner will use the LWOP log to ensure e-mail messages for all approved LWOP transactions in ILAM have been forwarded to the appropriate Pay and Compensation mailbox
		  • Pay and Compensation manager s will use the audit trail as required for reconciliation and audit purposes
		• The requirement for any reconciliation and review or audit procedures to be carried out by Pay and Benefits has not been addressed	

2.3 Internal Control Level Reporting	Management should report information on internal control levels and exceptions to the affected parties to ensure the continued effectiveness of its internal control system. Actions should be taken to identify what information is needed at a particular level of decision making.	See 2.2.	See 2.2.

APPENDIX B

CORRECTIVE ACTION PLAN

Submitted

By the

HUMAN RESOURCES DIRECTORATE

Response to Final Audit

December 6, 1999

Recommendation	Correction Action	Completion Date
1. Business Continuity and User Department Alternative Processing Back-up Procedures: Human Resources should: a) ensure that Production Control has developed and approved ILAM continuity plans that meet Human Resources business requirements; and b) develop and approve alternative-processing procedures (LWP and LWOP) that may be used in the event ILAM service is disrupted.	Agreed. Production Control is to develop ILAM continuing plans that meet HR business requirements. Back-up procedures already exist in case ILAM service is disrupted. The Human Resources Management Committee (HRMC) will be briefed on the proposed plan for ILAM service continuity.	February 30, 2000
2. Validation of Supervisors: Human Resources, being the ILAM business owners, should address the need to design and implement controls (preventative and detective) to ensure the validity of supervisors assigned to approve ILAM transactions. The level of controls must manage the risk to a level acceptable to Human Resources.	Agreed. As soon as Notes hierarchical naming is implemented in HC, we will be able to log all requests where add/delete transactions are approved by a different supervisor.	June 30, 2000

Recommendation	Corrective Action	Completion Date
3. Review Procedures (LWP and LWOP): a) Human Resources should develop and formalise review procedures based upon Health Canada's accepted risk level, that ensure the integrity of ILAM transactions (LWP) processed by PMIS. b) Pay and Benefits should develop and formalise review procedures, based upon Health Canada's accepted risk level, that ensure the integrity of ILAM transactions (LWOP) processed by Pay and Benefits personnel.	Agreed. HRMC will be briefed on the monitoring mechanisms for ILAM.	January 30, 2000
4. Processing Control Procedures (LWP, LWOP and Oracle archiving): a) Production Control should finish development of all ILAM - related control requirements (including action plans to resolve problems) that ensure accuracy and completeness of processing. These procedures should be fully documented and approved by Production Control management. b) Human Resources should develop and approve control processes required to ensure the accuracy and completeness of the receipt of e-mails in the Pay and Benefits mailboxes of approved ILAM requests (LWOP). c) Production Control, once formally assigned the responsibility by Human Resources, should develop, document and approve procedures to control and monitor the transfer of ILAM transactions to the Oracle archive database. d) Human Resources should assign responsibility for archiving LWOP logs and ensure processing requirements are documented and finalized by the responsible party.	This has all been finalized.	November 15, 1999

[illegible]	[illegible]	Completion Date
5. Privacy and supervisor privacy considerations: Human Resources should ensure ILAM training addresses privacy issues regarding the safeguarding by supervisors of any ILAM printouts of employee information.	Agreed. This is included in ILAM information sessions.	December 1, 1999
6. Error handling: Human Resources, being the ILAM business owner, should formally assign responsibility, and develop processes, for following up on: a) ILAM transactions rejected by PMIS; b) ILAM transactions rejected by Pay and Benefits; c) ILAM leave requests not acted upon by supervisors; d) and ILAM mail messages that are undeliverable.	Agreed. They are part of the ILAM administration tasks carried out by HRD PMIS/ILAM Administrator. Error-handling procedures are available.	December 1, 1999
Note: In a November 17, 1999, phone discussion, the ILAM business owner noted recommendations, 7 to 10 were addressed subsequent to issuance of the draft report. We have not reviewed the documentation to support these subsequent actions and therefore cannot comment on their completeness or effectiveness		
7. Notes security considerations: Human Resources should ensure ILAM training highlights the importance of security precautions users should take regarding access to their Notes and ILAM databases.	Agreed. Notes security is included in information sessions.	December 1, 1999
8. PMIS leave module access: Human Resources should ensure PMIS leave module access rights are updated to reflect ILAM security considerations.	Done.	November 15, 1999
9. Oracle and LWOP log rights: Human Resources should finalise access rights for the Oracle database and the LWOP log.	Done.	November 15, 1999

Recommendation	Corrective Action	Completion Date
10. ILAM access rights: Human Resouces should finalise (and formally communicate to Notes Operations) ILAM access rights for LAN personnel, Notes Operations personnel (NCR and regional), Production Control personnel and any other specialised access rights. Such access rights should be reviewed by the ILAM business owner on an as required basis.	Done.	November 15, 1999
11. Monitoring by Security and Other Violations: Production Control and HR Systems should finalise the process for monitoring and reporting specific ILAM security or other violations, that may impact upon the security of ILAM.	Agreement between HRD and IMSD which is being finalised now.	January 30, 2000

Health Canada / Santé Canada

Audit and Accountability Bureau

Bureau de la vérification et de la responsabilisation

RAPPORT DE VÉRIFICATION INTERNE

Contrôles et sécurité touchant le module interactif des congés et des présences (MICP)

15 décembre 1999

Canada

RAPPORT DE VÉRIFICATION INTERNE

Contrôles et sécurité touchant le module interactif des congés et des présences (MICP)

Le 15 décembre 1999

Vérification effectuée par la Direction de la vérification de Santé Canada

English version on the back.

N° de vérification A8113

Chronologie de la vérification

- Date du début des examens de vérification — 4 octobre 1999
- Date d'achèvement des examens de vérification — 25 octobre 1999
- Rapport de vérification préliminaire accepté par le Sous-ministre adjoint principal de la Direction générale des services de gestion — 9 décembre 1999
- Rapport de vérification final approuvé par le Président du Comité ministériel de la vérification et de l'évaluation — 15 décembre 1999

crédits

La vérification dont il est question ici a été effectuée par la firme **PricewaterhouseCoopers (PwC)** sous la direction de la Direction de la vérification interne (DVI). La directrice responsable du projet pour le Ministère était **Carolyn Jeffrey**, qui a travaillé sous la supervision générale de **Gordon Peters**, Directeur à la DVI. Voici la liste des membres de l'équipe de vérificateurs de **PwC** et la fonction de chacun :

David Prime, expert-conseil principal, chef d'équipe;

Lana Doxtator, membre associé, responsable de la vérification dans la RCN; et

Valerie Plaskacz, membre associé, chargé d'examiner le fonctionnement du MICP dans le cadre des essais à Montréal.

Table des matières

	Page
Introduction	1
Contexte	1
Méthodologie et critères de vérification	2
Aperçu du MICP	4
Constatations	5
Contrôles internes	6
Recommandations	13
Sécurité	15
Recommandations	17
ANNEXE A — Processus et objectifs CobiT et observations et évaluations	
ANNEXE B — Plan d'action correcteur présenté par la Direction des ressources humaines	

INTRODUCTION

Contexte

La Direction des ressources humaines de Santé Canada a mis au point un module interactif des congés et des présences (MICP) pour consigner sous forme électronique les données relatives aux congés et aux présences. C'est le groupe de Solutions d'applications ministérielles de réseau (SAMR) qui veille principalement sur son évolution. Les éléments suivants prennent en charge assistance et coordination :

(i) l'équipe technique du SIGP;
(ii) le service du contrôle de la production, qui se charge des liens avec le SIGP; et
(iii) le responsable des activités liées au MICP, à la Direction des ressources humaines, qui se charge des considérations relatives à la fonctionnalité.

Le responsable en question a demandé à la Direction de la vérification interne de procéder à une vérification en janvier 1999 pour déterminer si les contrôles essentiels existaient et fonctionnaient bien dans le système. Le rapport des vérificateurs comprenait plusieurs recommandations se rapportant aux contrôles internes. L'équipe de projet chargée du MICP a réagi aux recommandations du rapport dans un document intitulé « Plan d'action en réaction à la vérification du MICP », mis à jour le 10 septembre 1999. Le responsable du MICP a demandé à la Direction de la vérification interne de procéder à une deuxième vérification en octobre 1999.

Les objectifs de la vérification consistaient à examiner et à évaluer l'intégrité du module en question et les facettes de la sécurité qui l'entourent selon les paramètres énoncés ci-dessous, puis de faire rapport à ce sujet :

- la mesure dans laquelle la version actuelle du module et les liens avec Lotus Notes et le Système d'information de gestion du personnel (SIGP) fonctionnent comme prévu; et
- la mesure dans laquelle l'application est protégée contre les cas non autorisés de manipulation des données et d'accès au système.

L'examen portait sur le MICP et les liens avec le SIGP et la base de données Oracle. De même, elle englobait les éléments suivants :

- le traitement des données par le module, l'ensemble des liaisons électroniques et la sortie des données;
- les diverses facettes de la sécurité entourant l'accès aux données et la manipulation de celles-ci; et
- la conservation des copies de sauvegarde et la capacité de reprise à la suite d'une défaillance.

La vérification touchait uniquement la sécurité de l'application elle-même et non pas les autres couches de sécurité qui entrent en jeu, c'est-à-dire ce qui protège le réseau, le système d'exploitation, les installations matérielles et les télécommunications.)

L'examen s'est déroulé au pré Tunney, à Ottawa, là où étaient situés les bureaux de Santé Canada en octobre et en novembre 1999.

Au moment de la vérification, le MICP était à l'essai. Au 1er novembre 1999, le responsable du MICP n'avait pas encore résumé ni analysé les évaluations faites du projet pilote et du résultat obtenu à la suite des essais. Nous avons tout de même pu passer en revue les résultats sommaires des essais approfondis réalisés par l'équipe chargée du projet du MICP concernant l'exactitude du traitement des données entre le MICP et le SIGP, tests s'échelonnant sur trois jours, du 18 octobre 1999 au 29 octobre 1999 (quelque 270 opérations). De même, nous avons pu passer en revue les résultats de test consignés dans le registre des essais de réception du MICP.

Méthodologie et critères de vérification

L'étude a pris la forme suivante :

- des discussions tenues avec le personnel concerné des Ressources humaines (les responsables du MICP) et avec les responsables techniques du projet MICP/SIGP, y compris les membres de l'équipe du projet pilote de Montréal;
- un examen de la documentation se rapportant au projet; et
- l'observation d'un essai montrant les éléments de fonctionnalité intégrés au MICP pour ce qui touche les contrôles internes et la sécurité, en date d'octobre 1999, dans la RCN[1].

Le cadre « CobiT » (*Control Objectives for Information and Related Technology*), oeuvre de l'ISACF (*Information Systems Audit and Control Foundation*), a servi à l'élaboration des critères de vérification. Nous avons choisi d'appliquer cinq critères associés à deux éléments du cadre « CobiT ».

Élément CobiT	Critère CobiT	Objectif de contrôle de haut niveau CobiT
Exécution et soutien	**ES4** : Offrir un service ininterrompu	Les services de TI qui se révèlent nécessaires doivent être offerts. Il faut réduire au minimum les effets d'une panne majeure sur les activités en se dotant d'un plan fonctionnel de maintien des activités de TI qui a été mis à l'épreuve, qui concorde avec le plan général de maintien des activités et qui tient compte des exigences connexes.
Exécution et soutien	**ES5** : Garantir la sécurité des systèmes	L'information ne devrait pas pouvoir être utilisée, communiquée ou modifiée sans autorisation. Elle devrait être protégée contre l'éventualité de dommages ou de pertes grâce à des mesures logicielles régissant l'accès aux systèmes, aux données et aux programmes réservé aux utilisateurs autorisés.
Exécution et soutien	**ES10** : Gérer les problèmes et les incidents	Un système de gestion des problèmes — qui consigne et « traite » tous les incidents — devrait permettre de régler les problèmes et les incidents,

[1] Nous avions prévu d'observer une démonstration semblable sur les lieux du projet pilote de Montréal le 1er novembre 1999, mais en raison d'une défaillance du serveur au bureau de Montréal, cela n'a pu être fait.

		et de faire enquête sur leur cause.
Exécution et soutien	**ES11** : Gérer les données	Les données doivent demeurer complètes, exactes et valides de l'entrée au stockage, en passant par la mise à jour, grâce à une combinaison efficace de contrôles spécifiques et généraux exercés sur les opérations de TI.
Suivi	**S2** : Évaluer les contrôles internes et leur capacité	L'engagement que prend la direction d'assurer le suivi des contrôles internes, d'évaluer leur efficacité et de faire rapport périodiquement à leur sujet devrait permettre d'atteindre les objectifs des contrôles internes appliqués aux procédés de TI.

Pour un exposé détaillé des critères et des objectifs de la vérification, voir l'***Annexe A***.

Organisation du rapport

Le présent rapport comporte deux parties : d'abord, un aperçu de la situation qui démontre ce qu'il en est du MICP et, ensuite, les constatations. La partie sur les constatations comprend deux catégories : les contrôles internes (notamment les copies de sécurité et la capacité de reprise en cas de défaillance) et la sécurité.

L'***Annexe A*** renferme des observations détaillées sur les contrôles internes et la sécurité ainsi que l'évaluation que nous en faisons en prenant pour référence les critères du cadre « CobiT ».

APERÇU DU MICP

Le MICP — application Lotus Notes — permettra de consigner sous forme électronique les demandes de congé de tous les employés de Santé Canada qui ont accès à Lotus Notes. Dans chaque cas, l'employé visé doit accéder à Lotus Notes en inscrivant son mot de passe, son code d'identification de dossier personnel (CIDP) et sa date de naissance. La validation du CIDP et de la date de naissance dans le MICP se fait au moyen d'une comparaison avec l'information téléchargée depuis le SIGP. Une fois que l'employé a créé son profil dans le MICP, il peut accéder aux renseignements sur lui dans le système une fois la séance ouverte dans Lotus Notes. Il peut entrer dans le système à tout instant pour se renseigner plus à fond sur les congés, notamment les « soldes ».

L'employé « crée » la demande de congé qu'il transmet pour approbation au superviseur désigné. L'employé ne peut approuver sa propre demande. Si un superviseur désigné a déjà approuvé ou rejeté la demande de congé d'un employé, le superviseur peut remplir une demande de congé au nom de l'employé et transmettre celle-ci pour approbation à un autre superviseur. L'employé est informé de cette opération par le courriel du MICP.

C'est l'employé qui choisit le superviseur. Ni le MICP ni le SIGP n'a de contrôle pour valider la légitimité du superviseur. Une fois un superviseur initial désigné, l'employé peut choisir un autre superviseur. Le MICP ne met pas au courant le superviseur initial (qui n'est pas forcément le superviseur légitime) de la modification. Chaque superviseur a accès uniquement aux opérations qu'il a approuvées (ou recommandées) à l'égard de l'employé.

Les demandes approuvées de congé payé, pour l'année courante, seront transmises par voie électronique au CIGP toutes les nuits. Les données mises à jour du SIGP seront téléchargées toutes les nuits pour que les bases de données du MICP demeurent à jour. Si le SIGP rejette une demande approuvée dans le MICP, l'employé reçoit un message d'erreur. Les demandes approuvées pour la prochaine période financière seront stockées dans un fichier distinct du MICP, pour que le traitement puisse se faire dans le SIGP durant le passage au nouvel exercice.

Le traitement des demandes approuvées de congé sans solde relèvera de Paye et avantages sociaux à la suite d'un message de courriel généré par le MICP et transmis à une boîte aux lettres de Paye et avantages sociaux réservée au traitement des demandes provenant du MICP (et accessible uniquement au personnel de Paye et avantages sociaux). Le droit d'accéder à la boîte aux lettres pour les mises à jour est limité au personnel de la Production et aux gestionnaires de Paye et avantages sociaux. Les agents de Paye et avantages sociaux ont accès en mode lecture aux informations en question, par liste de paye.

Les demandes de congé (payé ou non) qui n'ont pas été approuvées ne demeurent pas dans le MICP. Aprés 15 jours, un message de rappel est transmis à l'auteur et au superviseur. Après 20 jours, la demande rejetée est supprimée du MICP. Toute demande n'ayant pas donné lieu à un suivi est supprimée au bout de 60 jours.

Le service du contrôle de la production exercera une surveillance sur le cycle nocturne de traitement par lots SIGP/MICP. Le responsable du MICP transmettra quotidiennement un résumé des opérations au service du contrôle de la production. La résolution des problèmes liée au processus SIGP/MICP sera coordonnée par le service du contrôle de la production, avec l'aide du personnel chargé des opérations sur Lotus Notes, des opérations relatives au SIGP, de la conception du MICP ou du responsable du MICP.

Toutes les opérations relatives aux congés sans solde approuvés seront inscrites dans un registre. Le registre des congés sans solde est en cours d'élaboration. Il servira à des fins d'archivage. De même, les Systèmes des ressources humaines s'en serviront pour veiller à ce que le traitement se fasse de manière exacte et complète du MICP aux boîtes aux lettres attitrées. Ainsi que du traitement assuré par le personnel de Paye et avantages sociaux.

Les demandes de congé payé approuvées seront archivées dans la base de données Oracle. La structure de la base de données est prête, mais l'interface est encore en cours d'élaboration. Les registres de congé sans solde seront archivés après douze mois dans une base de données de Lotus Notes.

En date du 1er novembre 1999, les résultats des essais pilotes (avec les feuilles d'évaluation) n'avaient pas encore été rassemblés ni analysés. Nous n'avons pas examiné dans le détail les résultats du projet pilote. En date du 1er novembre 1999, l'équipe chargée du MICP, qui en était encore à examiner les choses, n'avait pas encore approuvé les critères d'évaluation qui permettront au MICP de passer de l'étape de l'acceptation à celle de la production.

CONSTATATIONS

Voici un résumé des principales constatations tirées de l'examen. L'***Annexe A*** présente des observations détaillées et l'évaluation que nous avons faite des contrôles présents dans le MICP. Les préoccupations ou faiblesses signalées à l'***Annexe A*** sont indiquées par référence à la recommandation applicable ci-dessous.

Contrôles internes

Pour examiner les contrôles internes, nous avons passé en revue la documentation, interviewé des membres clés de l'équipe chargée du projet et observé une démonstration du MICP dans la RCN.

Sous la rubrique des contrôles internes, nous avons porté notre regard sur les copies de sauvegarde et la capacité de reprise dans le cas de défaillance. Nous avons par ailleurs étudié les contrôles internes exercés sur les données en nous reportant à cinq étapes : la préparation des données, l'entrée des données, le traitement des données, la sortie des données, le stockage et l'élimination des données.

Copies de sauvegarde et capacité de reprise en cas de défaillance

Le service des opérations sur Lotus Notes fait périodiquement des copies de sauvegarde des bases de données sur Lotus Notes, notamment celles du MICP. Les données du SIGP sont sauvegardées périodiquement, elles aussi, dans le cours normal des opérations du SIGP. Par ailleurs, le service du contrôle de la production a mis en place une procédure qui permet de mettre à jour le module des congés du SIGP tout juste avant le traitement des opérations du MICP.

Les plans de maintien des activités sur Lotus Notes et sur le SIGP sont en place. Le plan de continuité des activités du MICP n'est pas pleinement étayé. Il reste à le parachever. Le plan de maintien des activités devrait inclure des considérations relatives aux TI, ainsi que des directives de traitement d'appoint du ministère utilisateur à appliquer le temps que la fonction des services d'information rétablisse le service après une catastrophe ou une défaillance. Les considérations dont il faut tenir compte dans le plan de maintien des activités sont exposées à fond dans l'***Annexe A***, plus particulièrement à la partie ES4 : assurer un service ininterrompu.

Les autres questions relatives aux contrôles internes sont abordées suivant les cinq étapes dont il est question.

1. Préparation des données

La mise en place du MICP permettra d'améliorer l'entrée des données. Auparavant, les employés remplissaient un formulaire de demande de congé qu'ils remettaient pour approbation à un superviseur. Les demandes approuvées étaient transmises à Paye et avantages sociaux et inscrites à la main dans le module des congés du SIGP. Faute de temps et en raison de la charge de travail, les agents chargés d'inscrire les données ne pouvaient valider une grande part de l'information à inscrire. D'où les erreurs d'entrée de données. Avec le MICP, les employés inscrivent leurs propres demandes de congé directement dans le système. Ils peuvent ainsi vérifier immédiatement l'exactitude des données inscrites. Voilà qui concorde avec le principe fondamental selon lequel l'entrée des données doit se faire le plus près possible de la source d'information (en l'occurrence, l'employé). Avec le MICP, c'est la source d'information elle-même qui entre les données.

2. Entrée des données

De par sa conception, le MICP calque le formulaire initial, dont les employés et les superviseurs devaient vérifier l'exactitude des renseignements (genre de congé, CIDP correct, dates correctes). Une fois les données entrées, le SIGP a exécuté des contrôles de validation avant le traitement (calcul de la durée, employés à salaire horaire ou quotidien, autorisation de congé).

Le MICP et le SIGP permettent d'exercer des contrôles sur l'exactitude et l'exhaustivité des renseignements, et certains contrôles de validation[2]. Toutefois, il n'y a pas validation de la

[2] L'exactitude des soldes dans le MICP dépendra en partie de l'exactitude des droits établis dans le SIGP par Paye et avantages sociaux. Tout juste avant la mise en oeuvre du MICP, le responsable de l'activité a déjà déterminé qu'il faut s'assurer d'inscrire dans le SIGP toutes les demandes « en suspens » faites à la main.

légitimité du « superviseur » dans le MICP ou le SIGP. C'est une faiblesse importante du point de vue du contrôle, au sens où la demande de l'employé (ajout ou suppression) peut être approuvée par une personne qui n'est pas autorisée à le faire.

Dans le système manuel utilisé auparavant, même si le personnel de Paye et avantages sociaux ne vérifiait pas la signature ou le nom du superviseur, l'employé devait quand même faire signer par son superviseur un formulaire écrit. Le système manuel comportait au moins trois contrôles compensatoires qui ne sont pas présents dans le MICP. Ces trois contrôles compensatoires, qui permettaient de dissuader et de réduire au minimum le traitement d'opérations relatives à un congé injustement approuvé, étaient les suivants :

- l'employé est tenu d'obtenir une signature réelle, si bien que le fraudeur doit imiter lui-même la signature ou demander à quelqu'un qui n'est pas habile à le faire, de signer;
- l'employé sait que la demande de congé sera lue et remplie par un agent de Paye et avantages sociaux; et
- l'employé sait que Paye et avantages sociaux gardera le bout de papier.

Dans le MICP, l'employé peut désigner n'importe quelle personne à Santé Canada comme son superviseur. L'opération est traitée pendant la nuit dans le SIGP, et la mise à jour se fait le lendemain. Les employés ont la possibilité de présenter une opération injustement autorisée et sont même encouragés à le faire pour les raisons suivantes :

- l'employé n'est plus tenu de remettre un papier en bonne et due forme;
- l'employé saura que l'agent de Paye et avantages sociaux ne touchera plus son formulaire de demande de congé (du moins pas dans le cas des congés payés); et
- l'employé aurait raison de présumer que le MICP traitera des milliers de demandes[3]; il estimera que les probabilités de se faire prendre sont minimales.

À l'heure actuelle, ni le MICP, ni le SIGP, ni le processus général ne permet de réduire le risque ou de repérer les cas de traitement de demandes approuvées sans fondement dans le MICP et le SIGP.

Le **tableau 1** ci-dessous illustre les scénarios possibles dans le cas du traitement d'une demande approuvée sans fondement, expose les facteurs qui permettent actuellement qu'une telle chose se produise et énumère des exemples du genre de contrôle compensatoire qu'il faut envisager d'adopter. Comme c'est le cas pour tout système de contrôle important, les contrôles doivent gérer le risque à un niveau acceptable aux yeux de l'organisation. Le responsable de l'activité liée au MICP doit donc déterminer un niveau de risque acceptable. Ensuite, les contrôles appropriés doivent être conçus.

[3] Selon l'évaluation préliminaire de l'impact du projet, effectuée en janvier 1998, le MICP devrait générer un volume annuel de 157 850 opérations..

Tableau 1
Scénarios possibles : cas d'autorisations injustifiées

Cas possibles d'autorisations injustifiées	Facteurs	Contrôles compensatoires possibles
SCÉNARIO UN 1. L'employé présente à son superviseur une demande de congé de 10 jours qui est valable. 2. L'employé désigne un « superviseur » non autorisé (p. ex., un collègue) pour faire approuver la suppression de cette demande et faire approuver une nouvelle demande de congé de un jour. 3. L'employé se voit attribuer un nouveau superviseur avant la fin de l'année. 4. L'employé examine et approuve un solde de congé de fin d'année 5. L'employé reçoit une somme forfaitaire en contrepartie de 9 jours de vacances inutiles (même s'il a pris 10 jours de vacances).	a) L'employé peut désigner n'importe quel autre employé de Santé Canada comme étant son « superviseur »; b) La « légitimité » du superviseur n'est pas vérifiée dans le MICP ni dans le SIGP; c) L'employé ne sait peut-être pas que le MICP note l'identité de l'auteur de la demande et de celui qui l'approuve (et la recommande) et que ces renseignements figurent dans le dossier; d) Le MICP n'avise pas le premier superviseur du fait que l'employé n'a plus le même superviseur; e) Le service des ressources humaines n'a pas conçu de façons de déceler les activités inhabituelles, par exemple les changements fréquents de superviseurs ou les suppressions fréquentes liées aux opérations relatives aux congés payés; f) Le MICP n'avise pas un superviseur de la suppression d'une opération qui a déjà été approuvée; g) Un superviseur a seulement accès aux opérations détaillées d'un employé dont il était le superviseur (le superviseur a certes accès aux soldes nets de l'employé, mais ce sont là des renseignements sommaires qui ne mettent pas en valeur l'activité opérationnelle); et h) Les superviseurs ne sont pas tenus d'examiner ou d'approuver par écrit les soldes de congé des employés durant le processus d'examen de fin d'année.	a) Le service des ressources humaines pourrait veiller à ce que la formation au MICP mette en valeur le fait que le MICP consigne l'identité de tous les auteurs d'une opération et de toutes les personnes qui approuvent les opérations, et le fait que les registres en question sont conservés et examinés dans le cours normal des choses par la direction; b) Les superviseurs pourraient être avisés par courrier électronique du fait qu'un employé a désigné une autre personne comme étant son superviseur au sein du MICP, puis prendre les mesures qui s'imposent dans chacun des cas qui se présente; c) Le service des ressources humaines (et peut-être l'administrateur du projet de MICP) pourrait être avisé par courrier électronique du fait que l'employé a changé de superviseur aux fins du MICP, et se pencher d'une façon ou d'une autre sur le côté raisonnable de tels changements; d) Seul le superviseur attitré et l'agent de Paye et avantages sociaux de l'employé seraient autorisés à désigner un nouveau superviseur; e) Le service des ressources humaines pourrait vérifier, au hasard ou selon un procédé statistique quelconque, si les opérations de modification et de suppression dans le cas des superviseurs sont appropriées; f) Si le deuxième « superviseur » supprime une demande approuvée par le premier superviseur, le premier superviseur pourrait en être avisé par courrier électronique, si bien qu'il appartiendrait au superviseur de déterminer tout suivi qui s'impose; et g) Le service des ressources humaines pourrait s'assurer que les superviseurs sont bien conscients d'une chose : ils doivent savoir si les opérations et soldes relatifs aux congés des employés sont exacts et raisonnables, et ils doivent en assumer la responsabilité.
SCÉNARIO DEUX 1. L'employé présente au bon superviseur une demande de congé de 10 jours qui est valable (présumons que cette demande porterait à « zéro » le solde de l'employé). 2. L'employé désigne un « superviseur » non	Voir plus haut.	Voir plus haut.

Cas possibles d'autorisations injustifiées	Facteurs	Contrôles compensatoires possibles
autorisé (p. ex., un collègue) pour faire approuver la suppression d'une demande initiale et faire approuver une nouvelle demande de congé pour seulement deux jours. 3. L'employé se voit attribuer un nouveau superviseur. 4. L'employé présente une demande de congé de huit jours au nouveau superviseur, qui ne sait pas qu'il « manque » huit jours au solde de l'employé dans le MICP, solde qui devrait être « zéro ». 5. Le nouveau superviseur approuve la demande de congé de huit jours. 6. L'employé prend huit jours de congé additionnels (il n'a droit à aucun).		
SCÉNARIO TROIS Comme plus haut, mais dans le cas d'une demande de congé exigeant une approbation à deux niveaux ou plus.	Voir plus haut.	Voir plus haut.
SCÉNARIO QUATRE 1. L'employé présente au bon superviseur une demande de congé sans solde de trois mois. 2. L'employé désigne un « superviseur » non autorisé (p. ex., un collègue) pour faire approuver la suppression de cette demande et faire approuver une nouvelle demande de congé sans solde de deux mois. 3. L'employé prend un congé de trois mois, mais la paie n'est touchée que pour deux mois.	Voir plus haut, plus : a) Paye et avantages sociaux n'a pas conçu de façons de repérer l'activité inhabituelle dans le MICP, par exemple les changements fréquents de superviseurs ou les suppressions fréquentes liées aux opérations relatives aux congés sans solde.	Voir plus haut, plus : a) Paye et avantages sociaux pourrait vérifier, au hasard ou selon un procédé statistique quelconque, si les opérations de modification ou de suppression dans le cas des superviseurs appropriées.

Il existe des contrôles qui portent sur le traitement des erreurs (congés payés). Le SIGP ne traitera pas une opération provenant du MICP si celle-ci ne répond pas à ses critères de validation des données. Toutefois, il est possible que les erreurs ne soient pas corrigées et transmises à nouveau au MICP, puis, en dernière analyse, réintégrées au SIGP pour que le solde des congés soit mis à jour. Ni le MICP ni le SIGP ne déclenchent ou contrôlent la retransmission des opérations corrigées. Comme l'employé a intérêt à ne pas retransmettre une opération erronée (pour que son solde de congés demeure élevé), le superviseur doit le savoir si l'opération a été rejetée et savoir qu'il est responsable de s'assurer que les demandes de congé rejetées sont bel et bien corrigées et retransmises.

Les contrôles portant sur le traitement des erreurs (congés sans solde) relèveront de la responsabilité du gestionnaire de Paye et avantages sociaux. À notre connaissance, Paye et

avantages sociaux ne dispose pas de processus d'examen ou autre qui tienne compte des éléments suivants :

a) la validation ou la vérification (surtout la validation des superviseurs) des opérations relatives à un congé sans solde générées par le MICP; ou
b) la responsabilité de s'assurer que les demandes rejetées donnent lieu à un suivi approprié.

3. Traitement des données

Certains contrôles touchant le traitement des opérations du MICP (congés payés) sont déjà en place ou existent à titre d'essai; toutefois, il reste à mettre la dernière main aux procédures complètes et étayées qui permettraient de garantir un traitement exact et complet, en prévoyant notamment des plans d'action pour régler les problèmes en temps utile.

Le traitement des demandes de congé payé exige des contrôles et des procédures de traitement des données se rapportant aux activités suivantes :

- l'importation des données du MICP;
- le téléchargement des données du MICP dans le SIGP;
- le téléchargement des opérations erronées du SIGP;
- la piste de vérification menant au MICP; et
- le transfert des données du MICP à la base de données archivistique Oracle.

De même, le traitement des demandes de congé sans solde exige des contrôles et des procédures de traitement des données se rapportant aux activités suivantes :

- veiller à ce que les messages de courriel transmis dans les boîtes aux lettres réservées de Paye et avantages sociaux, pour les opérations approuvées, soient exacts et complets;
- veiller à ce que la piste de vérification ou le registre pour l'intégration des données dans le MICP soit exact et complet; et
- le transfert des données du MICP dans la base de données archivistique de Notes.

4. Sortie des données

Les contrôles sur la sortie des données sont en place, mais il faut mettre la dernière main à certaines procédures, notamment l'examen quotidien du registre de la piste de vérification et d'erreurs du MIPC par le responsable du MICP.

Les employés peuvent faire imprimer les renseignements qui les concernent dans le MICP et les sauvegarder au besoin. Les superviseurs peuvent aussi faire imprimer le résumé du MICP et un état détaillé des opérations pour lesquelles ils ont tenu lieu de superviseur. Les superviseurs devraient être conscients des considérations relatives à la protection des renseignements personnels au moment de faire cela.

L'accès aux renseignements sur les opérations relatives aux congés sur les soldes est contrôlé. Il n'y a pas longtemps encore, les rapports sommaires sur les congés du MICP étaient transmis annuellement aux employés, pour être examinés et signés.

Récemment, Santé Canada a déterminé que plutôt que de signer un tel rapport une fois par année, l'employé devait aviser Paye et avantages sociaux dans les 10 jours de toute opération ou de tout solde contesté. Si Paye et avantages sociaux n'est pas avisé dans les 10 jours, l'opération est considérée comme ayant été acceptée par l'employé. Les rapports sommaires sur les congés du MICP seront encore transmis une fois par année pour examen aux employés qui n'ont pas accès au MICP[4].

5. Stockage et élimination des données

Il existe des procédures de stockage et d'élimination des données qui permettent de gérer les données du MICP.

Les opérations relatives aux congés payés seront archivées dans la base de données Oracle. Leur gestion relèvera du service du contrôle de la production. Les opérations relatives aux congés sans solde seront archivées dans une base de données Notes dont la gestion relèvera du service des opérations sur Notes. Il faut encore parachever les procédures de gestion et de contrôle des activités d'archivage.

[4] C'est une politique qu'il faut envisager avec soin. Par exemple, il se peut très bien qu'un employé soit parti pendant plus de 10 jours. S'il ne dispose que de 10 jours pour corriger une erreur, il faut savoir si l'employeur ne disposerait lui aussi que de 10 jours pour corriger une erreur du MICP ou du SIGP (erreur administrative, fraude ou autre).

Recommandations

Sujet de la recommandation	*Recommandation(s)*
1) Procédures pour le maintien des activités et un procédé de traitement de sauvegarde des ministères utilisateurs	Les Ressources humaines devraient : a) veiller à ce que le service du contrôle de la production ait mis au point et approuvé des plans de maintien des activités du MICP qui répondent aux exigences des Ressources humaines; et b) mettre au point et approuver des procédures pour le traitement de rechange (congés payés et congés sans solde) qui serviraient au cas où le service du MICP serait interrompu.
2) Validation des superviseurs	Les Ressources humaines, responsables du MICP, devraient concevoir et mettre en place des contrôles (de prévention et de détection) pour garantir la validité des superviseurs chargés de l'approbation des opérations du MICP. Le niveau des contrôles doit permettre de gérer le risque selon un niveau acceptable aux yeux des Ressources humaines. Pour d'autres options, voir le **tableau 1**.
3) Procédures d'examen (congés payés et congés sans solde)	a) Les Ressources humaines devraient élaborer et officialiser des procédures d'examen fondées sur un niveau de risque acceptable pour Santé Canada, pour veiller sur l'intégrité des opérations du MICP (congés payés) traitées par le SIGP. b) Paie et avantages sociaux devrait élaborer et officialiser des procédures d'examen fondées sur un niveau de risque acceptable pour Santé Canada, pour veiller sur l'intégrité des opérations du MICP (congés sans solde) traitées par le personnel de Paie et avantages sociaux.
4) Procédures de contrôle du traitement (congés payés, congés sans solde et archivage dans Oracle)	a) Le service du contrôle de la production devrait parachever le développement de toutes les exigences de contrôle relatives au MICP (y compris les plans d'action conçus pour la résolution des problèmes) afin que le traitement soit à la fois exact et complet. Ces procédures devraient être pleinement étayées et approuvées par la direction du service de contrôle de la production. b) Les Ressources humaines devraient mettre au point et approuver les processus de contrôle requis pour garantir la réception exacte et complète des messages de courriel dans les boîtes aux lettres de Paie et avantages sociaux dans le cas des demandes approuvées du MICP (congés sans solde). c) Le service du contrôle de la production, une fois que les Ressources humaines lui attribuent officiellement la responsabilité, devrait mettre au point, étayer et approuver des procédures pour assurer le contrôle et le suivi du transfert des opérations du MICP dans la base de données archivistique Oracle. d) Les Ressources humaines devraient attribuer la responsabilité de l'archivage des registres concernant les congés sans solde et veiller à ce que la partie responsable étaye et parachève les exigences de traitement.
5) La protection des renseignements personnels et la discrétion du superviseur	Les Ressources humaines devraient s'assurer que la formation relative au MICP traite de la question de la protection des renseignements personnels, plus particulièrement du fait pour les superviseurs de protéger toute information imprimée du MICP à propos d'un employé.
6) Traitement des erreurs	Les Ressources humaines, responsables du MICP, devraient attribuer officiellement la responsabilité et élaborer des processus pour ce qui touche les

Sujet de la recommandation	*Recommandation(s)*
	éléments suivants : a) les opérations du MICP rejetées par le SIGP; b) les opérations du MICP rejetées par Paie et avantages sociaux; c) les demandes de congé du MICP auxquelles les superviseurs n'ont pas donné suite; et d) les messages de courrier du MICP qui ne sont pas distribuables.

Sécurité

Les contrôle de sécurité sont dictés en partie par le degré de sensibilité des données, et établi par une classification formelle des données. Les données du MICP sont classées « Protégées B », à l'instar des renseignements du SIGP.

Il existe des contrôles qui visent à restreindre l'accès non autorisé aux renseignements du MICP. Pour accéder au MICP, il faut le mot de passe de l'employé dans Lotus Notes avec les contrôles déjà en place sur l'identification, l'authentification et l'accès, que gère le groupe chargé des opérations sur Lotus Notes. Toutefois, les contrôles en question sont compromis dans la mesure où l'employé ne protège pas son mot de passe ou n'utilise pas la fonction F5, qui exige la réinscription du mot de passe de Notes, lorsqu'il s'éloigne de son ordinateur.

Le responsable du MICP a communiqué en bonne et due forme les profils d'accès au groupe des opérations sur Notes pour le projet pilote, mais la version finale des profils d'accès du MICP reste être transmisse. Les profils en question devraient énoncer notamment les exigences relatives à l'accès (dans les régions et à la RCN) pour le groupe des opérations sur Notes, le service du contrôle de la production, les Ressources humaines et Paie et avantages sociaux.

Chaque employé a accès seulement à ses propres renseignements dans le MICP. Les superviseurs peuvent accéder aux renseignements dans le MICP concernant les employés pour lesquels ils sont désignés comme étant « superviseur ». Cela donne un aperçu du solde de l'employé, des précisions sur les opérations à l'égard desquelles ils ont agi comme superviseur et la possibilité d'entrer une demande au nom de l'employé. Dans les cas où le superviseur entre une demande au nom de l'employé, l'employé en est automatiquement avisé grâce aux messages de courriel générés par le MICP.

L'accès au module des congés est géré par l'agent de sécurité du SIGP. À l'heure actuelle, l'accès est autorisé pour le personnel de Paie et avantages sociaux, le personnel du service du contrôle de la production et divers membres du personnel dans les régions (en raison des contraintes imposées au personnel de Paie et avantages sociaux) et dans la RCN (Division de la politique et des services consultatifs, Direction générale des services médicaux, Direction générale des services de gestion et bureaux de la direction). Avant la mise en oeuvre du MICP, et de façon permanente, le caractère approprié et nécessaire de l'accès au SIGP devrait être examiné, tout comme les conséquences pour le MICP.

Notes permet d'exercer un contrôle sur certaines transgressions des paramètres de sécurité dans les bases de données comme le MICP. Le service du contrôle de la production et les Systèmes des ressources humaines auront pour responsabilité de contrôler ces activités. Jusqu'à maintenant, les indicateur n'ont pas été définis. Exemples des activités pouvant être l'objet d'un contrôle : les cas où un utilisateur essaie d'ouvrir une session en Notes en tapant, disons, quatre mots de passe erronés. Ou encore : l'utilisateur essaie plusieurs fois d'approuver sa propre opération.

Recommandations

Sujet de la recommandation	*Il est recommandé de:*

Nota : Au cours d'une discussion téléphonique qui a eu lieu le 17 novembre 1999, le responsable du MICP a noté que les recommandations 7 à 10 ont été prises en considération après la production d'un rapport préliminaire. Nous n'avons pas examiné la documentation qui permettrait d'étayer les mesures ainsi prises subséquemment; par conséquent, nous ne pouvons dire si elles sont complètes ou efficaces.

7) Considérations relatives à la sécurité de Notes	Les Ressources humaines devraient s'assurer que la formation relative au MICP souligne l'importance pour les utilisateurs de prendre des précautions en ce qui concerne l'accès à leurs bases de données sur Notes et du MICP.
8) Accès au module des congés du SIGP	Les Ressources humaines devraient s'assurer de mettre à jour les droits d'accès au module des congés du SIGP pour tenir compte des considérations relatives à la sécurité du MICP.
9) Droits touchant Oracle et le registre des congés sans solde	Les Ressources humaines devraient préciser les droits touchant l'accès à la base de données Oracle et au registre des congés sans solde.
10) Droits touchant l'accès au MICP	Les Ressources humaines devraient parachever (et communiquer officiellement au service des opérations sur Notes) les droits concernant l'accès au MICP dans le cas du personnel des réseaux locaux, du personnel du service des opérations sur Notes (dans la RCN et dans les régions), du personnel du service de contrôle de la production. Il en va de même de tous autres droits d'accès spécialisés. Le responsable du MICP devrait examiner au besoin de tels droits d'accès.
11) Contrôle des paramètres de sécurité et des cas de transgression	Le service du contrôle de la production et les Systèmes des ressources humaines devraient parachever le processus de contrôle et de signalement des cas de transgression des règles de sécurité ou autres du MICP, dans la mesure où cela a une incidence sur la sécurité du MICP.

ANNEXE A

Processus et objectifs CobiT
et
Observations et évaluations

Le tableau suivant décrit nos observations et notre évaluation des contrôles du MICP. En ce qui concerne l'examen de la fiabilité de l'interface SIGP/MICP, nous avons effectué plusieurs transactions MICP au cours de l'essai mené dans la RCN, et, le lendemain, nous avons examiné les journaux de traitement SIGP/MICP, les écrans SIGP et les résumés MICP mis à jour. Nous avons vérifié si nos essais de transaction ont été traités (ou non, si la transaction visait le prochain exercice ou si elle a été rejetée par le SIGP) dans le SIGP. Même si, en date du 1er novembre 1999, les résultats des essais n'avaient pas été reçus, analysés et examinés par l'équipe chargée du projet MICP, nous avons été en mesure de passer en revue les résultats d'ensemble des essais détaillés de la mise à jour de MICP/SIGP effectués par l'équipe chargée du projet MICP au cours d'une période de trois jours, du 18 au 29 octobre 1999 (environ 270 transactions). Puisque l'interface avec la base de données Oracle n'est pas encore établie, nous n'avons pas pu examiner les contrôles touchant le transfert de dossiers de MICP à Oracle. Le journal de vérification des CSS est en cours d'élaboration, de sorte que nous n'avons pas été en mesure de déterminer si le journal est exact, complet et utile.

La vérification s'attache uniquement à la sécurité des applications et ne tient pas compte de la sécurité sur l'ensemble de l'infrastructure, comme le réseau, le système d'exploitation, les installations physiques et les télécommunications.

L'évaluation et les observations suivantes sur les contrôles sont fondées sur les éléments suivants :

- Entrevues et discussions avec les personnes suivantes :

David Windsor	Contrôle de la production (base de données Oracle)
Lizabeth Gray	Adjointe du chef du projet MICP
John Campeau	Opérations sur Notes
Darquise Gauthier	Développateur (MICP)
Joanne Chartrand	Responsable de la sécurité, SIGP
Donald Constantineau	Contrôle de la production
Sylvie Bouillon	Chef de projet (SIGP)
Pauline Thériault	Chef de projet (MICP)

- Démonstration MICP effectuée le 8 octobre 1999 par Pauline Thériault; et
- Examen de
  - divers documents, registre, rapports et notes de service fournis par les personnes interrogées;
    divers documents, résultats d'essais, notes de service, rapports et registre contenus dans le guide de travail, la base de données sur la formation, la base de données d'aide et le registre des essais de réception sur MICP; et

rapports de vérification antérieurs, de documents de travail et de réponses des membres de l'équipe MICP aux recommandations de la vérification.

Élément CobiT	Objectifs de contrôle	Observation	Notre évaluation
ES4 Exécution et soutien : Assurer la continuité du service			
4.3 Contenu du Plan de continuité des technologies de l'information	Les gestionnaires des services d'information devraient veiller à ce qu'on élabore un plan s'assortissant des éléments suivants : • identification des applications, des services dispensés par des tierces parties, des systèmes d'exploitation, du personnel et des fournitures , ainsi que des fichiers de données critiques et des délais nécessaires au rétablissement après un désastre; • lignes directrices sur l'utilisation du plan de continuité; • procédures de rétablissement permettant de ramener les activités au niveau où elles étaient avant l'incident ou le désastre; • procédures pour protéger et reconstruire le site principal; • procédures de communication avec les parties concernées, y compris les employés et la direction; • identification de solutions de rechange concernant le site de relève et le matériel informatique, et sélection d'une des solutions. Le cas échéant, un contrat officiel pour l'obtention de ces services devrait être conclu; et • information essentielle sur les équipes responsables de la continuité, sur le personnel concerné, sur les clients, sur les fournisseurs, sur les autorités publiques et sur les médias. Les gestionnaires des services d'information devraient établir des procédures et des lignes directrices afin de réduire au minimum les exigences de continuité touchant le personnel, les installations, le matériel informatique, les logiciels, l'équipement, les formulaires, les fournitures et les meubles.	• Il existe des plans de continuité pour Notes et pour le module des congés de SIGP. • Opérations sur Notes produira tous les jours, toutes les semaines et tous les mois des copies de sauvegarde des bases de données Notes dans la RCN. Les fichiers quotidiens sont conservés pendant huit semaines, et les bandes hebdomadaires et mensuelles sont conservées indéfiniment. • Les services Opérations sur Notes régionaux sont responsables de la production de copies de sauvegarde en région, et cette responsabilité est énoncée en détail dans la version des Rôles et responsabilités liés à MICP qui a été produite en septembre 1999 (*Ce document aurait apparemment été terminé le 4 novembre 1999*). Il faut signaler que la production de copies de sauvegarde des serveurs Notes régionaux n'est peut-être pas nécessaire, si la démarche de duplication n'est plus valide. • On produit des copies de sauvegarde SIGP immédiatement avant le traitement SIGP/MICP; cette pratique s'ajoute à la production régulière de copies de sauvegarde SIGP. • Le plan de continuité pour le module MICP n'a pas encore été élaboré, documenté et approuvé.	On n'a pas encore élaboré, documenté et approuvé un Plan de continuité des opérations pour MICP. ***(Voir la recommandation 1)***

ANNEXE A

Processus et objectifs CobiT
et
Observations et évaluations

[illegible]	[illegible]	[illegible]	[illegible]
4.5 Maintenir le Plan de continuité des technologies de l'information	Les gestionnaires des services d'information devraient prévoir l'établissement de procédures de contrôle du changement afin de veiller à ce que le plan de continuité soit à jour et reflète les exigences opérationnelles actuelles. Cela suppose que les procédures de mise à jour du plan de continuité reflètent les changement et les procédures touchant la gestion et les ressources humaines. Les gestionnaires des services d'information devraient établir des procédures permettant de dresser un « bilan », de façon à pouvoir évaluer l'efficacité du plan après la reprise des activités des services d'information à la suite d'un désastre, et à apporter les correctifs qui s'imposent.	Le plan de continuité relatif au MICP n'a pas encore été élaboré, de sorte qu'on n'a pas tenté d'établir des procédures spécifiques de contrôle du changement.	***(Voir la recommendation 1)***

ANNEXE A

Processus et objectifs CobiT
et
Observations et évaluations

Élément CobiT	Objectif de contrôle	Observation	Évaluation
4.6 Plan de continuité des technologies de l'information — Formation et essais	La méthodologie de continuité en cas de désastre devrait prévoir que toutes les parties concernées assisteront à des séances de formation régulières concernant les procédures à suivre advenant un incident ou un désastre. Pour assurer l'efficacité du plan de continuité, la direction doit l'évaluer régulièrement, ce qui suppose une préparation soignée, l'obtention de documentation et de résultats d'essais, et la mise en oeuvre d'un plan d'action à la lumière des résultats obtenus.	Puisque le plan de continuité du MICP n'a pas encore été élaboré, les exigences touchant la formation et les essais n'ont pas été définies.	***(Voir la recommendation1)***
4.8 Plan de continuité des technologies de l'information — Diffusion	Compte tenu de la nature confidentielle de l'information contenue dans le plan de continuité, ce document devrait être distribué uniquement au personnel autorisé et devrait être protégé contre la divulgation non autorisée. Par conséquent, chaque section du plan doit être diffusé uniquement aux personnes qui ont besoin de l'information.	Les restrictions touchant la diffusion du plan de continuité n'ont pas encore été définies.	***(Voir la recommendation 1)***
4.9 Solutions de sauvegarde pour le traitement par les ministères utilisateurs	La méthodologie de continuité devrait veiller à ce que les ministères utilisateurs établissent des procédures de traitement de sauvegarde susceptibles d'être utilisées jusqu'à ce que les services d'information soient en mesure de rétablir pleinement le service après un désastre ou un événement.	Si le MICP est en panne, les employés devraient être tenus de recourir aux méthodes de traitement manuelles. Les Ressources humaines n'ont pas encore documenté les exigences et l'incidence du recours aux méthodes manuelles pour toutes les parties concernées (c'est.-à-dire) les employés, les superviseurs, Paie et avantages sociaux, etc.).	Cette question n'a pas encore été abordée. (***Voir la recommendation 1***)

ANNEXE A

Processus et objectifs CobiT et Observations et évaluations

EA4 Exécution et aide : Assurer la sécurité des systèmes			
5.2 Identification, reconnaissance et accès	L'accès logique aux ressources informatiques des services d'information, ainsi que leur utilisation, devrait être limité grâce à la mise en place de mécanismes convenables de reconnaissance des utilisateurs identifiés et de ressources liées aux règles régissant l'accès. De tels mécanismes préviendraient l'accès aux ressources informatiques : • par des employés non autorisés; • au moyen de connexions non autorisées par ligne commutée; et • par d'autres systèmes (réseaux) non autorisés. De tels mécanismes devraient aussi réduire au minimum le besoin d'attribuer plusieurs codes d'accès aux utilisateurs autorisés. Il faudrait aussi établir des procédures permettant d'assurer l'efficacité des mécanismes de reconnaissance et d'accès (p. ex., changements réguliers de mots de passe).	**MICP :** --Accès pour tous les employés ministériels dotés d'un profil dans Notes, par l'entremise d'un profil par défaut pour tous les employés ministériels. --Pour accéder au MICP la première fois, l'employé doit entrer son mot de passe pour Notes, ainsi que son CIDP et sa date de naissance (le MICP confirme le CIDP et la date de naissance grâce à l'information provenant du SIGP) --Par la suite, l'employé n'a plus qu'à entrer son mot de passe pour Notes pour accéder au MICP. --Seul l'employé et son superviseur ont accès à l'information touchant l'employé. --Le contrôle des mots de passe dans le MICP est assuré grâce à Lotus Notes --La tentative d'accéder à Lotus Notes n'entraîne pas une révocation du droit d'accès, mais la consignation répétée de mots de passe erronés entraîne le ralentissement progressif de l'accès à Notes — la vitesse de traitement retourne à la normale lorsque le bon mot de passe est consigné --Même si Opérations sur Notes tient un journal des tentatives répétées d'accès au système, on n'examine ce journal que sur demande. --La formation relative au MICP devrait signaler aux employés qu'ils doivent toujours utiliser la touche F5 pour bloquer l'accès à Lotus Notes (et, par conséquent, au MICP). --On peut, grâce à Notes, accéder au MICP par réseau commuté --Le MICP ne permet d'accéder à aucune autre application — les transactions MICP sont téléchargées dans le SIGP grâce à un processus de traitement différé des lots. **SIGP :** --Les droits d'accès sont contrôlés par Joanne Chartrand — des contrôles rigoureux des mots de passe et de l'accès au SIGP empêchent l'accès non autorisé --À l'heure actuelle, plusieurs employés n'appartenant pas aux RH (surtout dans les régions) ont accès au SIGP pour modifier les données touchant les congés. --Une sélection de programmeurs peuvent accéder au système par réseau commuté --Le SIGP est doté d'un pare-feu	On court le risque que des personnes non autorisées accèdent à l'information MICP d'un employé. (***Voir les recommandations 7 et 10***) On court le risque que des personnes non autorisées modifient des transactions MICP dans le SIGP. (***Voir la recommendation 8***)

ANNEXE A

Processus et objectifs CobiT
et
Observations et évaluations

5.3 Sécurité de l'accès aux données en direct	En ce qui concerne les technologies de l'information en direct, les gestionnaires des services d'information devraient adopter des procédures, conformes à la politique de sécurité, qui permettent de contrôler l'accès en fonction du besoin prouvé d'une personne de consulter, d'ajouter, de modifier ou d'effacer des données.	--On a établi des profils de sécurité MICP pour le projet pilote, l'accès a été offert aux utilisateurs, aux administrateurs du serveur Notes et au contrôle de la production — les profils de sécurité finaux (dans la RCN et en région) à utiliser lorsque le MICP est en production n'ont pas été approuvés et parachevés par le client, et ils n'ont pas été soumis à Opérations sur Notes en vue de fournir l'accès au MICP par l'entremise de Notes (*on nous a donné à croire que ces profils ont été terminés après les travaux de préparation pour la présente vérification.*) --L'accès aux fichiers MICP suppose la consignation initiale d'une date de naissance et d'un CIDP valides, et l'accès subséquent est limité aux utilisateurs et aux superviseurs assignés --Cependant, rien ne permet de déterminer si la personne qui approuve la demande de congé est effectivement le superviseur de l'employé concerné.	Les profils de sécurité MICP pour tous les groupes doivent être établis et présentés à Opérations sur Notes **(Voir la recommendation 10)** Une demande de congé présentée dans le MICP peut être créée ou effacée par un superviseur non autorisé. ***(Voir la recommendation 2)***
5.4 Gestion des comptes d'utilisateurs et revue des comptes d'utilisateurs par les gestionnaires	Les gestionnaires devraient établir des procédures favorisant la prise de mesures en temps opportun pour la demande, l'établissement, l'émission, la suspension et la fermeture de comptes d'utilisateurs. Ces procédures devraient s'assortir d'une méthode d'approbation officielle énonçant les données ou nommant le propriétaire du système qui accorde les privilèges d'accès. Les gestionnaires devraient créer un processus de contrôle permettant de passer en revue et de confirmer périodiquement le droit d'accès.	Joanne Chartrand gère l'accès des utilisateurs au SIGP, et elle examine périodiquement le droit d'accès des utilisateurs. --Notes ID gère l'attribution de mot de passe/privilège d'"accès pour toutes les applications Lotus Notes, en fonction des demandes de changement soumises par l'entremise du service de dépannage --Le personnel d'Opérations sur Notes de la RCN, certains employés d'Opérations sur Notes des régions et le personnel de Paie et avantages sociaux doivent jouir d'un droit d'accès aux listes de paie pertinentes dans le MICP. L'exploitant du MICP doit examiner périodiquement les droits d'accès afin de s'assurer qu'ils sont nécessaires et appropriés. (*Un tel processus n'a pas encore été établi à la fin de nos travaux préparatoires. On nous a laissé croire que le processus a maintenant été établi.)* --L'accès des utilisateurs au MICP se limite à l'information sur leurs propres congés. Il n'y a pas lieu d'examiner la question de l'accès général pour chaque utilisateur.	Il existe un processus de gestion de l'accès au SIGP, mais ce processus devrait tenir compte de l'incidence sur le MICP. ***(Voir la recommendation 8)*** L'accès au MICP devrait être achevé officiellement et communiqué à Opérations sur Notes. ***(Voir la recommendation 10)***
5.6 Contrôle des comptes d'utilisateurs par les utilisateurs	Les utilisateurs devraient contrôler systématiquement l'activité touchant leur(s) compte(s). Il faudrait aussi établir des mécanismes d'information leur permettant d'assurer le suivi de l'activité normale et de repérer rapidement les activités inhabituelles.	Chaque employé peut assurer un suivi quotidien. De plus : • les employés sont immédiatement avisés des demandes refusées par les superviseurs; • les employés et les superviseurs sont avisés de toute erreur de traitement du SIGP le jour suivant; • les employés sont avisés de toute demande de congé présentée en leur nom par un superviseur; et • chaque employé est tenu de signaler toute anomalie à Paie et avantages sociaux dans les 10 jours qui suivent la transaction.	L'utilisateur peut examiner et contrôler l'activité sur le MICP qui le concerne, mais cet examen et ce contrôle sont limités par une récente décision stratégique de Santé Canada qui exige que les employés avisent Paie et avantages sociaux de toute anomalie dans les 10 jours suivant la transaction. ***(Voir la recommendation11)***

ANNEXE A

Processus et objectifs CobiT et Observations et évaluations

Élément CobiT	Objectif CobiT	Observations	Note
5.7 Suivi de sécurité	Les administrateurs de la sécurité des services d'information devraient veiller à ce que les activités de sécurité soient consignées dans un registre et à ce que tout indice de violation imminente de la sécurité soit signalé immédiatement à l'administrateur et fasse l'objet de mesures automatiques.	• Opérations sur Notes tient un registre des tentatives d'accès à Notes. On peut examiner la liste des tentatives d'accès, sur demande. • Opérations sur Notes peut repérer les tentatives d'accès et autres « violations » (p. ex., tentatives d'un utilisateur de recourir à une fonction non autorisée) dans les applications Notes. De telles violations seront examinées par Contrôle de la production et Systèmes de DRH. • Le MICP n'est pas doté d'exigences de contrôle ou de limites touchant les tentatives d'accès et les « violations » dans le MICP. • On n'a pas tenté de déterminer si de telles exigences de contrôle seraient utiles ou faisables.	L'exploitant du MICP n'a pas établi d'exigences officielles de surveillance de sécurité. (***Voir la recommandation 11***).
5.8 Classement des données	Les gestionnaires devraient établir des procédures pour veiller à ce que toutes les données soient classées, en fonction du niveau de confidentialité, au moyen d'une décision officielle et explicite par le propriétaire des données, selon une méthode de classement des données. Même les données qui n'exigent « aucune protection » devraient faire l'objet d'une décision officielle leur attribuant une telle désignation .	Les données du MICP sont classées à titre d'information Protégée B, tout comme les données du SIGP.	Les données ont été classées à titre d'information Protégée B. Par conséquent, l'accès aux données du MICP est limité à l'employé et au superviseur.
5.9 Gestion centrale de l'identification des droits d'accès	Il existe des mesures de contrôle permettant de veiller à ce que l'identification et le droit d'accès de l'utilisateur, ainsi que l'identité du système et du propriétaires des données, soient établis et gérés centralement afin d'assurer l'uniformité et l'efficience du contrôle global de l'accès.	Le mot de passe Lotus Notes permet d'accéder uniquement au MICP. Les données téléchargées du MICP au SIGP sont traitées en différé chaque soir. L'accès au SIGP est contrôlé et suivi.	L'accès au MICP ne permet pas d'accéder à d'autres applications.

ANNEXE A

Processus et objectifs CobiT et Observations et évaluations

Objectif CobiT	Objectifs de contrôle	Observations	Note d'risque
5.10 Rapports sur les violations et les activités de sécurité, et traitement des incidents	Les administrateurs de la sécurité des services d'information devraient veiller à ce que les violations et les activités de sécurité soient consignées, signalées, examinées et soumises aux autorités supérieures appropriées de façon régulière, afin de repérer et de mettre un terme aux activités non autorisées. L'accès logique à l'information redditionnelle touchant les ressources informatiques (sécurité et autres registresjournaux) devrait être attribué en fonction du principe du moindre privilège ou du besoin de savoir. La direction devrait établir un mécanisme de traitement des incidents touchant la sécurité informatique afin de résoudre les problèmes de sécurité grâce à une plate-forme centralisée offrant une expertise suffisante et des installations de communication rapides et sûres. Il faudrait établir les responsabilités et les procédures touchant la gestion des incidents afin de veiller à ce que des mesures de sécurité efficaces et appropriées soient prises en temps opportun.	Voir 5.7	Voir 5.7
5.12 Ré-accréditation	La direction devrait procéder à une ré-accréditation périodique afin d'assurer la mise à jour du niveau de sécurité officiellement approuvé et d'accepter le risque résiduel.	Voir 5.7	Voir 5.7
5.15 Non-répudiation	La politique organisationnelle devrait veiller, lorsqu'il est approprié de le faire, à ce que les transactions ne puissent être répudiées par les parties concernées, et à ce que des mesures de contrôle soient mises en oeuvre afin d'assurer la non-répudiation de l'origine ou de la réception, de la preuve de présentation et de la réception des transactions.	• Les activités de l'auteur et du superviseur sont consignées dans chaque transaction du MICP, dans la piste de vérification, dans les copies de sauvegarde MICP conservées indéfiniment par Opérations sur Notes, ainsi que dans les archives Oracle, pendant sept ans. • Il est possible que les utilisateurs nient avoir consigné de l'information ou approuvé une transaction et prétendent qu'un autre utilisateur a accédé à leur information sur Notes et, par conséquent, à leur information sur le MICP. Le risque est faible, car de telles allégations pourraient être rejetées par la politique ministérielle qui prévoit la confidentialité des mots de passe Notes, le changement périodique des mots de passe Notes, l'utilisation de la touche F5 par l'employé pour empêcher l'accès à Notes lorsqu'il s'absente et la directive selon laquelle les employés doivent examiner périodiquement leurs transactions MICP et de signaler les anomalies à Paie et avantages sociaux.	Il faudrait réduire au minimum la possibilité que les utilisateurs répudient les transactions. (***Voir la recommendation 7***)

ANNEXE A

Processus et objectifs CobiT et Observations et évaluations

	Objectifs de contrôle	Observation	
ES10 Exécution et service : Gérer les problèmes et les incidents			
10.1 Système de gestion des problèmes, échelle de résolution des problèmes et piste de vérification	Les gestionnaires des services d'information devraient définir et mettre en oeuvre un système de gestion des problèmes permettant : • la consignation, l'analyse et la résolution en temps opportun de tout événement opérationnel qui ne s'inscrit pas dans le fonctionnement régulier (incidents, problèmes et erreurs). Des rapports d'incidents devraient être établis lorsqu'il s'agit d'un problème considérable; • la résolution rapide et efficiente des problèmes repérés. Ces procédures devraient favoriser l'établissement de priorités appropriées. Les procédures devraient aussi documenter l'échelle de résolution des problèmes pour l'activation du plan de continuité des technologies de l'information. • Le système de gestion des problèmes devrait offrir une piste de vérification adéquate permettant de remonter jusqu'à la cause fondamentale (p. ex., mise en place d'un ensemble d'applications ou mise en oeuvre d'un changement urgent). Il devrait être lié étroitement à la gestion du changement, de la disponibilité et de la configuration.	CP • Le processus de traitement différé (le soir) de l'information SIGP/MICP est géré par Contrôle de la production • Des méthodes provisoires permettant de composer avec les problèmes de traitement SIGP/MICP sont décrites en détail dans les Rôles et responsabilités de Soutien technique. • On n'a ni documenté, ni approuvé, ni achevé des procédures détaillées permettant de résoudre des problèmes opérationnels pendant le traitement SIGP/MICP. CSS • L'exploitant du MICP sera responsable de veiller à ce que toutes les demandes de CSS approuvées dans le MICP occasionnent l'envoi d'un message à Paie et avantages sociaux. Ce processus n'a pas été élaboré, et il en va de même pour les processus permettant de résoudre les problèmes (*Une discussion avec l'exploitant du MICP nous a permis de constater que ces processus sont considérés comme nécessaires : ils ne seront donc pas élaborés (sic).)*	Les événements opérationnels (liés aux CP et au traitement MICP/SIGP) qui ne s'inscrivent pas dans le fonctionnement régulier sont consignés par Opérations de production. Toutefois, les procédures (provisoires) touchant l'analyse et la résolution de ces problèmes n'ont été ni pleinement documentées, ni officiellement approuvées par la direction de Contrôle de la production. (***Voir la recommandation 4***) On n'a pas encore envisagé la question d'un système de gestion des problèmes qui s'attacherait au problème de traitement touchant les transactions de CSS. (***Voir la recommandation 4***)

Processus et objectifs CobiT
et
Observations et évaluations

[illegible]	Objectifs de contrôle	Observations	[illegible]
ES11 Exécution et service : Gérer les données			
11.1 Méthodes de préparation de données	Il faudrait établir des contrôles et des méthodes de préparation de données, y compris les éléments suivants : • formulaire de consignation de données, pour réduire au minimum les erreurs et les oublis; • autorisation du document source, y compris la répartition adéquate des tâches; • méthodes de dépouillement du document source, pour s'assurer que l'information est complète et exacte; • méthodes de traitement des erreurs; • définition des exigences de conservation du document source.	--Les données sont consignées directement dans le MICP par l'employé, il n'y a aucun formulaire de consignation d'information, et le MICP vérifie diverses variantes, y compris les dates de début/fin pour les employés nommés pour une période déterminée. ----L'employé a l'occasion de vérifier les données avant de les soumettre à l'approbation de son superviseur. --Dans certains cas, un superviseur peut présenter une demande de congé pour l'employé; le superviseur a l'occasion de vérifier l'information avant de la soumettre à l'approbation d'une tierce partie, et l'employé aura l'occasion de confirmer l'information de la transaction lorsqu'il recevra un message par courriel concernant la transaction effectuée en son nom. --On réduit au minimum les possibilités d'erreur de date, car l'employé sélectionne les dates à partir d'un calendrier. --Méthodes de dépouillement du document source pour s'assurer que l'information est complète : processus permettant de veiller à ce que les transactions rejetées par le SIGP ou les transactions qui n'ont toujours pas été approuvées par le MICP fassent l'objet d'un suivi approprié. --Même si les superviseurs et les employés reçoivent des rappels par courriel concernant les demandes non approuvées qui sont laissées en suspens dans le MICP, la responsabilité en ce qui concerne la prise de mesures de suivi appropriées n'a pas été officiellement attribuée. --Exigences relatives à la conservation du document source — voir 11.19	Les contrôles touchant la préparation de données se sont améliorés, grâce à la consignation d'information directement provenant de la source. Il est possible que des transactions soient approuvées par des personnes qui ne sont pas autorisées à le faire. ***(Voir la recommandation 2)*** La conception des méthodes de traitement des erreurs n'est pas encore terminée. ***(Voir la recommandation 6)***

Processus et objectifs CobiT
et
Observations et évaluations

11.2 Consignation de données : Autorisation	Il faudrait établir des contrôles et des méthodes pour la consignation de données et prévoir que : • la classification de données ne devrait être effectuée que par le personnel autorisé.	***Autorisations*** Contrôles notés pour la consignation de données : --Chaque employé est autorisé à consigner des données sur les congés dans le MICP, les transactions ne peuvent être autorisées par l'employé qui présente la demande. --Les employés peuvent accéder uniquement à leur propre compte MICP. --Les superviseurs peuvent accéder uniquement à leur propre compte MICP, et au compte des employés pour lesquels ils sont le superviseur assigné. --Si un superviseur présente une demande de congé au nom d'un employé assigné, l'employé est avisé de la demande par l'entremise de Notes, et ce dernier peut prendre des mesures au besoin (c.-à-d. communiquer avec le superviseur, avec Paie et avantages sociaux, etc.). --Un superviseur qui présente une demande au nom d'un employé assigné ne peut autoriser la transaction : l'autorisation doit être obtenue auprès d'une tierce partie. --Les tentatives de soumettre des demandes de congé plus long que le solde des jours de congé ne sont pas acceptées. --L'utilisateur ne peut accéder qu'au profil MICP des employés pour lesquels il est le superviseur assigné (c.-à-d. qu'un utilisateur ne peut consulter les données MICP concernant un autre employé, même s'il connaît son CIDP et sa date de naissance). --Les transactions consignées dans le MICP comprennent l'identité de la personne qui présente la demande, de celle qui en recommande l'acceptation et de celle qui l'approuve. --Points faibles au chapitre du contrôle de la consignation des données : --La consignation de données pourrait être approuvée par des superviseurs non autorisés, car il n'existe aucun contrôle dans le MICP et le SIGP. --Des personnes non autorisées pourraient accéder aux bases de données Notes d'un employé ou d'un superviseur, y compris à l'information consignée dans le MICP.	Des utilisateurs non autorisés pourraient accéder au dossier d'un employé ou d'un superviseur sur Notes (et, par conséquent, au MICP). (***Voir la recommendation 7***) Les superviseurs ne sont pas reconnus dans le MICP et le SIGP (***Voir la recommendation 2***).

Processus et objectifs CobiT
et
Observations et évaluations

11.7 Consignation de données : exactitude, exhaustivité et validité	Il faudrait établir des contrôles et des méthodes de consignation de données, et veiller notamment à ce que : • les données de transaction consignées (par des personnes, par le système ou au moyen d'une interface) en vue d'être traitées font l'objet de contrôles variés pour vérifier l'exactitude, l'exhaustivité et la validité de l'information.	<u>Consignation de données — Contrôles remarqués</u> —Des contrôles de validation ont déjà été établis dans le SIGP, et on continue de les utiliser (comprend la vérification de l'existence, de l'exhaustivité et (ou) de l'exactitude des éléments suivants : type de transaction, exercice financier, CIDP, bureau de paie, mois du congé, code de congé, date du début, date de la fin, période d'emploi, indicateur de durée — heures ou jours, semaine de travail variable/semaine normale de travail, ajout/effacement d'information sur le sommaire d'utilisation des congés). --Le MICP effectue plusieurs contrôles de validation des données consignées (y compris la validation des éléments suivants : date, CIDP, date de naissance, code de congé, semaine de travail comprimée, type de transaction, calcul de la durée, solde des congés). --Le MICP invite l'utilisateur à soumettre un certificat médical, conformément aux exigences du contrat; tout comme dans la méthode manuelle, c'est au superviseur qu'il incombe d'assurer le suivi en ce qui concerne les attestations de médecins. --Le MICP calcule la durée du congé. --Le MICP avise l'employé que la demande de CSS approuvée a été acheminée à Paie et avantages sociaux. --Le SIGP effectue la plupart des vérifications de validité, tel que mentionné plus haut — dans le SIGP, le processus de validation comprend la recherche de demandes identiques. --Paie et avantages sociaux sera chargé de veiller à ce que tous les soldes de congé soient à jour avant de commencer la mise en oeuvre. <u>Consignation de données — Points faibles remarqués</u> —Aucune validation des personnes qui approuvent ou qui recommandent — l'employé peut assigner tout autre employé comme superviseur. --Même si le nom du « superviseur » non autorisé serait consigné dans l'information sur le congé, seul l'employé aurait accès à ces renseignements — le vrai superviseur ne pourrait consulter cette information, car il ne peut accéder qu'aux transactions pour lesquelles il est le superviseur assigné. --Une demande approuvée par le superviseur n° 1 peut être effacée par le superviseur n° 2 (sans que le superviseur n° 1 n'en soit avisé).	Les contrôles visant à vérifier l'exactitude et l'exhaustivité des données consignées sont convenables. Les contrôles visant à vérifier la compétence de la personne qui approuve ne sont pas convenables. (***Voir la recommendation 2***)

Processus et objectifs CobiT
et
Observations et évaluations

[illegible]	[illegible]	[illegible]	[illegible]
11.8 Consignation de données : Traitement des erreurs	Il faudrait établir des contrôles et des méthodes de consignation des données comprenant l'élément suivant : • Correction d'informations erronées et consignation de nouveaux renseignements corrigés.	--Si le SIGP refuse une transaction (approuvée par le superviseur dans le MICP) qui comporte une erreur, l'auteur de la demande reçoit le jour suivant un message expliquant l'erreur. --On a déterminé que c'est à l'employé qu'il incombe de corriger la demande rejetée par le SIGP (qui avait été approuvée dans le MICP). --C'est au superviseur que devrait revenir la responsabilité de veiller à ce qu'une demande de congé corrigée soit consignée, approuvée et enregistrée afin de refléter tout congé réellement pris (rien n'incite l'employé à présenter une nouvelle demande). --Les transactions rejetées sont effacées du MICP après 20 jours. --Le superviseur qui approuve une demande ne sera au courant de la transaction rejetée que s'il examine le dossier de l'employé au cours des 20 jours qui suivent le rejet de la demande et remarque le statut de la transaction dont il est question, ce qui est improbable.	Les méthodes et les contrôles permettant de corriger l'information et de présenter une demande corrigée ne sont pas complètes. (***Voir la recommandation 6***)

Processus et objectifs CobiT
et
Observations et évaluations

Numéro CobiT	Objectifs de contrôle	Observations	Évaluations
11.9 Traitement de données : Intégrité, validation et révision	Il faudrait définir des contrôles en matière de traitement de données qui comprendraient les éléments suivants : • maintien de la répartition des tâches; • mise en place de contrôles adéquats des mises à jour, comme des totaux de contrôle séquentiels et des contrôles de la mise à jour du fichier maître; et • validation, reconnaissance et révision le plus près possible du point d'origine.	**CP** • Le traitement est distinct de la consignation de données -- les transactions dans le MICP sont traitées en lots différés (processus géré par le Contrôle de la production). • Le Contrôle de la production a élaboré des méthodes préliminaires pour l'analyse et l'examen quotidiens de l'examen du cycle d'activités qui se répète tous les soirs (y compris l'exportation de données du MICP, la réception des données par le SIGP, le traitement par le SIGP et la mise à jour subséquente du MICP) -- (*même si ces méthodes n'étaient ni documentées ni complétées au moment de nos travaux préparatoires, on nous a donné à croire qu'elles étaient terminées.*) • Il faut élaborer des méthodes permettant de satisfaire aux exigences touchant le traitement et la résolution de problèmes liés à l'importation de données du SIGP, à la téléexportation de données du MICP au SIGP, à la téléimportation de transactions et de pistes de vérification erronées du SIGP dans le MICP. **CSS** • Le traitement est distinct de la consignation de données — la demande est soumise par l'employé et approuvée par le superviseur, et la demande approuvée est traitée par Paie et avantages sociaux. • L'accès à la boîte aux lettres de Paie et avantages sociaux est limité de la façon suivante : les gestionnaires peuvent mettre l'information à jour, et les autres employés de Paie et avantages sociaux peuvent consulter l'information. • L'exploitant du MICP n'a pas terminé l'élaboration de méthodes pour l'examen quotidien de l'exactitude et de l'exhaustivité des messages par courriel transmis à Paie et avantages sociaux. • L'élaboration des procédures d'examen qui doivent être appliquées par Paie et avantage sociaux n'est pas terminée. **Remarque :** Avant le lancement du MICP, l'exploitant a établi un processus permettant de veiller à ce que les soldes des congés dans le SIGP soient à jour.	Même s'ils ont pour la plupart déjà été rédigés, les contrôles touchant le traitement de données (CP) dans le SIGP/MICP n'ont été ni pleinement documentés, ni approuvés. (***Voir la recommandation 4***) Les contrôles visant le traitement de données sur le CSS n'ont été ni élaborés, ni documentés, ni approuvés. (***Voir la recommandation 4***) L'élaboration des procédures d'examen qui doivent être appliquées par Paie et avantages sociaux n'est pas terminée. (***Voir la recommandation 3)***

Processus et objectifs CobiT
et
Observations et évaluations

[illegible]	[illegible]	[illegible]	[illegible]
11.11 Traitement de données : Traitement des erreurs	Il faudrait définir les contrôles pour le traitement de données comprenant ce qui suit : • des procédures de traitement des erreurs qui permettent aux transactions erronées d'être repérées sans être traitées et sans interrompre le traitement de transactions valides.	CP • Les demandes de CP approuvées sont traitées dans le cadre du cycle de traitement en lots du SIGP/MICP, et les demandes refusées restent dans le MICP pendant 20 jours, période après laquelle elles sont effacées — les demandes qui ne sont pas approuvées n'influent aucunement sur le traitement en temps opportun des demandes non approuvées (sic). • Les demandes approuvées par le MICP et rejetées par le SIGP ne sont pas traitées par le SIGP : elles sont enregistrées dans la piste de vérification, et l'auteur de la demande reçoit un avis de rejet par courriel. • Les messages d'erreurs numériques ont été traduits en messages d'erreurs textuels qui seront acheminés aux employés en guise de suivi (*au moment de nos travaux préliminaires, l'examen final et l'approbation de ces messages d'erreurs visant à fournir des renseignements appropriés à l'employé et à Paie et avantages sociaux n'étaient pas terminés. On nous a donné à croire que les travaux ont été terminés depuis.*) • On n'a pas élaboré de processus visant à s'assurer que tous les messages d'erreurs font l'objet d'un suivi, et la responsabilité à cet égard n'a pas été assignée. • L'élaboration d'un processus permettant de veiller à ce que toutes les demandes qui n'ont pas été approuvées fassent l'objet d'un suivi approprié n'a pas été envisagée. CSS • Paie et avantages sociaux traite les demandes de CSS approuvées sur réception d'un message par courriel généré par le MICP. • Les demandes qui n'ont pas été approuvées restent dans le MICP pendant 20 jours, période après laquelle elles sont effacées — les demandes non approuvées n'influent pas sur le traitement en temps opportun des demandes approuvées. • L'élaboration d'un processus visant à s'assurer que toutes les demandes non approuvées font l'objet d'un suivi approprié n'est pas terminée.	Les contrôles touchant le traitement des erreurs n'ont été ni pleinement documentés, ni approuvés. (***Voir la recommandation 6***)

Processus et objectifs CobiT
et
Observations et évaluations

[illegible]	[illegible]	[illegible]	[illegible]
11.12 Distribution des extrants : Traitement, sécurité et conservation, distribution, mise en concordance, examen des extrants et traitement des erreurs	Il faudrait définir des contrôles et des procédures concernant les extrants qui comprendraient les éléments suivants : • distribution et sécurité des extrants, y compris la distribution de copie papier et électronique; • pistes de vérification et procédures permettant de veiller à ce que les extrants soient toujours comparés aux totaux pertinents; et • vérification de l'exactitude des extrants, y compris des procédures de contrôle des erreurs contenues dans les extrants.	Distribution et sécurité des extrants • Les employés peuvent imprimer et conserver l'information contenue dans leur dossier, s'ils estiment qu'il est nécessaire de le faire. • Les superviseurs peuvent imprimer et examiner les transactions de l'employé et le solde des congés — les gestionnaires doivent être au courant des enjeux liés à la sécurité et à la protection des renseignements personnels. • Le personnel de Paie et avantages sociaux peut imprimer et examiner l'information contenue dans le MICP et le SIGP — le personnel de Paie et avantages sociaux connaît les exigences en matière de protection des renseignements personnels en ce qui concerne l'information contenue dans les dossiers. Pistes de vérification et procédures de mise en concordance — contrôle de processus 4 CP • Contrôle de la production utilise les pistes de vérification pour s'assurer que les extrants du SIGP correspondent aux transactions contenues dans le MICP — l'élaboration de ces procédures n'est pas terminée. CSS • Les travaux d'élaboration du journal de vérification des demandes de CSS et les méthodes permettant de mettre en concordance les transactions effectuées dans le MICP et les messages par courriel reçus par Paie et avantages sociaux ne sont pas terminés. (Remarque : la responsabilité concernant ces processus sera probablement attribuée au futur administrateur de projet MICP.) Examen des extrants, y compris les procédures touchant le contrôle des erreurs —voir 2.2	Il faudrait envisager l'adoption de lignes directrices à l'intention des superviseurs sur les enjeux en matière de protection des renseignements personnels et les exigences d'examen. (***Voir la recommendation 5***) Il faut terminer l'élaboration des procédures de traitement de Contrôle de la production. (***Voir la recommendation 4***) Il faut terminer l'élaboration de procédures visant à s'assurer que les transactions (CSS) MICP reçues par Paie et avantages sociaux sont complètes. (***Voir la recommendation 4***)

Processus et objectifs CobiT
et
Observations et évaluations

Objectif CobiT	Objectif de contrôle	Observation	Note de service
11.19 Gestion de la mémoire	Il faudrait élaborer des procédures relatives à la mise en mémoire qui tiennent compte des exigences touchant l'extraction de données, de la rentabilité et de la politique de sécurité.	• Les transactions MICP seront téléchargées dans la base de données Oracle lorsque les critères suivants sont respecté: : la transaction est âgée de plus de 12 mois, elle a été approuvée et elle a été acceptée par le SIGP. • Les dossiers contenus dans la base de données Oracle seront conservés pendant sept ans. • L'élaboration de procédures touchant la gestion et le contrôle de l'accès à l'information archivée dans Oracle n'est pas terminée. • Les détails concernant les transactions CSS approuvées dans le MICP seront consignés dans le registre CSS (ce journal est en cours d'élaboration). • L'élaboration des procédures concernant la gestion et le contrôle de l'accès au registre CSS n'est pas terminée. (*On nous a donné à croire que seuls Paie et avantages sociaux et le groupe administratif du MICP auront accès au registre CSS.)* • L'information sera conservée dans le registre CSS pendant un an, et sera ensuite archivée dans une base de données Lotus Notes et conservée pendant sept ans.	Il faudrait finir l'élaboration de procédures touchant la mise en mémoire pour les activités d'archivage dans Oracle et de consignation d'informations dans le journal de CSS. (***Voir la recommandation 9***)
11.23 Copies de sauvegarde et restauration	Les gestionnaires devraient mettre en oeuvre une stratégie appropriée pour la production de copies de sauvegarde et la restauration afin de veiller à ce qu'elles s'assortissent d'un examen des exigences opérationnelles et de l'élaboration, de la mise en oeuvre, de la mise à l'essai et de la documentation d'un plan de redressement. Il faudrait établir des procédures permettant de veiller à ce que les copies de sauvegarde respectent les exigences opérationnelles. Il faudrait établir des procédures permettant de veiller à ce que les copies de sauvegarde respectent la stratégie établie à cette fin et à ce que l'on vérifie régulièrement que les copies de sauvegarde sont utilisables.	Voir 4.3	Voir 4.3
11.24 Production de copies de sauvegarde	Il faudrait établir des procédures permettant de veiller à ce que les copies de sauvegarde respectent la stratégie établie à cette fin et à ce que l'on vérifie régulièrement que les copies de sauvegarde sont utilisables.	Voir 4.3	Voir 4.3
11.26 Archivage	Les gestionnaires devraient établir une politique et des procédures permettant de veiller à ce que les archives respectent les exigences juridiques et opérationnelles et soient convenablement protégées et enregistrées.	Voir 11.19	Voir 11.19

Processus et objectifs CobiT
et
Observations et évaluations

S2 Déterminer si les contrôles internes sont adéquats				

2.2	Contrôles internes en temps opportun	L'utilisation de contrôles internes suppose que ces derniers repèrent rapidement les erreurs et les anomalies et comprennent des mesures correctives avant qu'elles ne minent la production et l'exécution. L'information touchant les erreurs, les anomalies et les exceptions devrait être conservée et systématiquement soumise aux gestionnaires.	• Il n'existe pas de procédures concernant le signalement des erreurs, des anomalies et des exceptions aux gestionnaires.
			
			CP
			• Pendant le projet pilote, Contrôle de la production fournissait aux RH un résumé quotidien des transactions MICP (les RH utilisaient les résumés pour suivre le volume des transactions pendant le projet pilote).
			• L'élaboration d'un modèle pour un tel rapport après la mise en oeuvre n'est pas terminée.
			• Pendant le projet pilote, Contrôle de la production a conçu une version plus détaillée de la piste de vérification et l'a soumise à l'examen (volume seulement) de l'exploitant.
			  • La version initiale ne comprenait pas le nom de la personne qui fournit son approbation — cet oubli a été corrigé dans les versions subséquentes.
			  • L'exploitant du MICP doit se pencher sur la question des exigences touchant la forme, le contenu et la « lisibilité » de la piste de vérification quotidienne des transactions CP, et Contrôle de la production doit établir de telles exigences.
			• Un tel rapport devrait mettre en relief ou indiquer les transactions MICP « inhabituelles » (c'est-a-dire coûteuses ou autres).
			  • Exemples de type d'information qu'un tel rapport pourrait signaler aux RH : nombre de transactions effacées, nombre de transactions rejetées, nombre de cas où le superviseur a apporté plus de trois modifications au cours du dernier mois (ou autre critère similaire).
			• Un tel rapport de Contrôle de la production pourrait être utilisé par l'exploitant du MICP (probablement le futur administateur de projet MICP) dans le cadre d'un examen du contrôle interne.
			• Exemples de type d'information qu'un tel rapport pourrait signaler aux RH : nombre de transactions effacées, nombre de transactions rejetées, nombre de cas où le superviseur a apporté plus de trois modifications au cours du dernier mois (ou autre critère similaire)
				Il est possible qu'une erreur systématique ou une défaillance des contrôles ne soit pas portée à l'attention des cadres supérieurs. (***Voir la recommendation 2***)

2.2 Contrôles internes en temps opportun (suite)		CSS
		• Le personne de Paie et avantages sociaux sera responsable d'élaborer les méthodes d'examen des demandes CSS approuvées — l'élaboration de ces procédures n'est pas terminée.
		• On élabore actuellement un rapport de piste de vérification pour les transactions CSS.
		• Seul l'exploitant du MICP et les gestionnaires de Paie et avantages sociaux auront accès au registre CSS.
		  • L'exploitant du MICP utilisera le journal CSS pour s'assurer que les messages par courriel pour toutes les transactions CSS approuvées dans le MICP ont été acheminées à la bolte aux lettres appropriée de Paie et avantages sociaux.
		  • Les gestionnaires de Paie et avantages sociaux utiliseront la piste de vérification à des fins de rapprochement et de vérification, tel qu'exigé.
		• Le besoin d'adopter des procédures touchant le rapprochement et l'examen ou la vérification par Paie et avantages sociaux n'a pas été envisagé.	

2.3 Niveau de contrôle interne	Les gestionnaires devraient divulguer l'information sur les niveaux de contrôle interne et les exceptions aux parties concernées afin d'assurer l'efficacité continue de son système de contrôle interne. Des mesures devraient être prises pour déterminer quelle information doit être fournie à un niveau décisionnel donné.	Voir 2.2.	Voir 2.2.

ANNEXE B

PLAN D'ACTION CORRECTEUR

présenté par

LA DIRECTION DES RESSOURCES HUMAINES

Réponse à la vérification finale

Le 6 décembre 1999

Recommandation	Mesures correctives	Délai
1. <u>Procédures pour le maintien des activités et un procédé de traitement de rechange des ministères utilisateurs</u> Les Ressources humaines devraient : a) veiller à ce que le service du contrôle de la production ait mis au point et approuvé des plans de maintien des activités du MICP qui répondent aux exigences des Ressources humaines; et b) mettre au point et approuver des procédures pour le traitement de rechange (congés payés et congés sans solde) qui serviraient au cas où le service du MICP serait interrompu.	Entendu. Le service du contrôle de la production doit mettre au point des plans de maintien des activités du MICP qui répondent aux exigences des Ressources humaines. Des procédures de sauvegarde existent déjà pour l'interruption du service du MICP. Le comité de gestion des ressources humaines sera renseigné sur le plan proposé pour la continuité du service du MICP.	Le 30 février 2000 (sic)
2. <u>Validation des superviseurs</u> Les Ressources humaines, responsables du MICP, devraient concevoir et mettre en place des contrôles (de prévention et de détection) pour garantir la validité des superviseurs chargés de l'approbation des opérations du MICP. Le niveau des contrôles doit permettre de gérer le risque selon un niveau acceptable aux yeux des Ressources humaines.	Entendu. Dès que la désignation hiérarchique en Notes est mise en place à Santé Canada, nous pourrons enregistrer toutes les demandes de modification ou de suppression d'opérations qui sont approuvées par un superviseur différent.	Le 30 juin 2000

Recommandation	Mesures correctives	Délai
2. Procédures d'examen (congés payés et congés sans solde) a) Les Ressources humaines devraient élaborer et officialiser des procédures d'examen fondées sur un niveau de risque acceptable pour Santé Canada, pour veiller sur l'intégrité des opérations du MICP (congés payés) traitées par le SIGP. b) Paie et avantages sociaux devrait élaborer et officialiser des procédures d'examen fondées sur un niveau de risque acceptable pour Santé Canada, pour veiller sur l'intégrité des opérations du MICP (congés sans solde) traitées par le personnel de Paie et avantages sociaux.	Entendu. Le comité de gestion des ressources humaines sera renseigné sur les mécanismes de contrôle mis en place pour le MICP.	Le 30 janvier 2000

[illegible]	[illegible]	[illegible]
4. <u>Procédures de contrôle du traitement (congés payés, congés sans solde et archivage dans Oracle)</u> a) Le service du contrôle de la production devrait parachever le développement de toutes les exigences de contrôle relatives au MICP (y compris les plans d'action conçus pour la résolution des problèmes) afin que le traitement soit à la fois exact et complet. Ces procédures devraient être pleinement étayées et approuvées par la direction du service de contrôle de la production. b) Les Ressources humaines devraient mettre au point et approuver les processus de contrôle requis pour garantir la réception exacte et complète des messages de courriel dans les boîtes aux lettres de Paie et avantages sociaux dans le cas des demandes approuvées du MICP (congés sans solde). c) Le service du contrôle de la production, une fois que les Ressources humaines lui attribuent officiellement la responsabilité, devrait mettre au point, étayer et approuver des procédures pour assurer le contrôle et le suivi du transfert des opérations du MICP dans la base de données archivistique Oracle. d) Les Ressources humaines devraient attribuer la responsabilité de l'archivage des registres concernant les congés sans solde et veiller à ce que la partie responsable étaye et parachève les exigences de traitement.	Tout cela a été fait.	Le 15 novembre 1999
5. <u>La protection des renseignements personnels et le superviseur</u> Les Ressources humaines devraient s'assurer que la formation relative au MICP traite de la question de la protection des renseignements personnels, plus particulièrement du fait pour les superviseurs de protéger toute information imprimée du MICP à propos d'un employé.	Entendu. Cela est compris dans les séances d'information sur le MICP.	Le 1er décembre 1999

Recommandation	Mesures correctives	Date
6. Traitement des erreurs Les Ressources humaines, responsables du MICP, devraient attribuer officiellement la responsabilité et élaborer des processus pour ce qui touche les éléments suivants : a) les opérations du MICP rejetées par le SIGP; b) les opérations du MICP rejetées par Paie et avantages sociaux; c) les demandes de congé du MICP auxquelles les superviseurs n'ont pas donné suite; et d) les messages de courrier du MICP qui ne sont pas distribuables.	Entendu. Cela fait partie des tâches administratives du MICP qui relèvent de l'administrateur du SIGP/MICP de la Direction des ressources humaines. Il existe des procédures pour le traitement des erreurs.	Le 1er décembre 1999
Nota : Au cours d'une discussion téléphonique qui a eu lieu le 17 novembre 1999, le responsable du MICP a noté que les recommandations 7 à 10 ont été prises en considération après la production d'un rapport préliminaire. Nous n'avons pas examiné la documentation qui permettrait d'étayer les mesures ainsi prises subséquemment; par conséquent, nous ne pouvons dire si elles sont complètes ou efficaces.		
7. Considérations relatives à la sécurité de Notes Les Ressources humaines devraient s'assurer que la formation relative au MICP souligne l'importance pour les utilisateurs de prendre des précautions en ce qui concerne l'accès à leurs bases de données sur Notes et du MICP.	Entendu. La question de la sécurité de Notes fait partie des séances d'information.	Le 1er décembre 1999
8. Accès au module des congés du SIGP Les Ressources humaines devraient s'assurer de mettre à jour les droits d'accès au module des congés du SIGP pour tenir compte des considérations relatives à la sécurité du MICP.	C'est fait.	Le 15 novembre 1999
9. Droits touchant Oracle et le registre des congés sans solde Les Ressources humaines devraient préciser les droits touchant l'accès à la base de données Oracle et au registre des congés sans solde.	C'est fait.	Le 15 novembre 1999

Recommandation	Mesure corrective	Date
10. Droits touchant l'accès au MICP Les Ressources humaines devraient parachever (et communiquer officiellement au service des opérations sur Notes) les droits concernant l'accès au MICP dans le cas du personnel des réseaux locaux, du personnel du service des opérations sur Notes (dans la RCN et dans les régions), du personnel du service de contrôle de la production. Il en va de même de tous autres droits d'accès spécialisés. Le responsable du MICP devrait examiner au besoin de tels droits d'accès.	C'est fait.	Le 15 novembre 1999
11. Contrôle des paramètres de sécurité et des cas de transgression Le service du contrôle de la production et les Systèmes des ressources humaines devraient parachever le processus de contrôle et de signalement des cas de transgression des règles de sécurité ou autres du MICP, dans la mesure où cela a une incidence sur la sécurité du MICP.	La DRH et la DSGI ont conclu à ce sujet un arrangement auquel on met actuellement la touche finale.	Le 30 janvier 2000